North Dakota
Homeland Security
Anti-Terrorism Summary

The North Dakota Open Source Anti-Terrorism Summary is a product of the North Dakota State and Local Intelligence Center (NDSLIC). It provides open source news articles and information on terrorism, crime, and potential destructive or damaging acts of nature or unintentional acts. Articles are placed in the Anti-Terrorism Summary to provide situational awareness for local law enforcement, first responders, government officials, and private/public infrastructure owners.

NDSLIC Disclaimer

Quick Links

North Dakota

Judge grants access to private land in Fargo-Moorhead for flood diversion study. A judge has given Cass County's joint water board in Fargo, North Dakota a permit to access land it had been unable to study along the route of a proposed Red River diversion project in the Fargo and Moorhead, Minnesota, area. The five families who own the eight parcels targeted by the civil litigation had refused to let engineers on their property to test the soil and survey for cultural artifacts, wetlands impact and hazardous materials. More than 800 acres are subject to the judge's ruling. Plots covered by the court-issued permit are in essential areas where the proposed floodwater bypass channel would cross rivers, said one of the co-managers of the Army Corps of Engineers study of the diversion. The proposed $1.5 billion diversion project would provide long-term flood control for the metro area, though some landowners downstream worry it might worsen the flood threat for them. Fargo-area residents have spent the last two springs battling major floods, including a record-setting crest in 2009 that damaged hundreds of homes, and forced thousands to evacuate. One of the arguments raised by landowners at an August 9 hearing on the access dispute was that the diversion was being hastily approved. The judge said in his order that it was not "the time or place for these arguments" concerning the project itself, and that the sole issue was whether granting access to the land was proper. Landowners will be paid $250 for each hole drilled for soil testing, as well as for any damage to crops. Source: http://www.bismarcktribune.com/news/state-and-regional/article_cab5a10a-b114-11df-9e0c-001cc4c03286.html

N.D. developing regional emergency response teams. North Dakota is undergoing an upgrade process to better prepare emergency response units in four regions and eight cities, including Jamestown. “We feel from the state of North Dakota that we are very fortunate to have these professional-level partners,” said a southeast regional response coordinator with the North Dakota Department of Emergency Services. Jamestown is considered a sub-level city in the southeast region with Fargo acting as the anchor city. Grand Forks anchors the northeast with Devils Lake as a sub. Bismarck anchors the southwest with Dickinson as a sub and Minot anchors the northwest with Williston as a sub. Although each anchor or sub is expected to respond to emergencies in its region, sometimes the response from others may be closest. One example would be Jamestown to Foster County, which is in the northeast region. All eight cities are near completion for the first of three phases. Phase one is emergency response resources for chemical, biological, radioactive, nuclear and explosive threats. Source: http://www.jamestownsun.com/event/article/id/117834/

Anthrax cases reported in North Dakota county. North Dakota’s agriculture department on August 24 said more cases of anthrax had been confirmed in cattle. The new cases were in Pembina County. Earlier cases were confirmed in Barnes, Dickey and Sioux counties, all in the southern half of the state. State animal health officials are continuing to urge ranchers to have cattle vaccinated against the disease. Anthrax bacteria spores lie dormant in the ground and become active under conditions such as heavy rainfall, flooding or drought. North Dakota usually has a few anthrax cases in cattle every year. Source: http://www.businessweek.com/ap/financialnews/D9HQ01IO0.htm

GFK loses power Wednesday night; flights on time this a.m. An electrical outage forced the Grand Forks International Airport in North Dakota, to use generators to light runways and power the air-traffic control tower as a passenger flight landed late August 18, an airport official said. The airport's lead operations specialist said passengers exited the plane on the tarmac rather than leave through the main terminal, which lost power and does not have generators. He said the power went out shortly after 10 p.m. August 18, and, after repairs, the power was restored at about 4:30 a.m. August 19. All flights departed on time the morning of August 19. Source: http://www.grandforksherald.com/event/article/id/172576/group/homepage/

REGIONAL

(Minnesota) **Alert for Sudden Death Syndrome in soybean.** Conditions have been conducive for Sudden Death Syndrome (SDS) in crops this year, and the Southern Research and Outreach Center in Waseca, Minnesota, reports SDS is more common this year in the Waseca area than ever before. SDS has the potential to lead to significant soybean yield losses, with documented losses ranging from 5 to 70%. As of June 2010, SDS has been confirmed in 23 Minnesota counties. Originally the disease was concentrated in south central Minnesota, but it could potentially occur almost anywhere in the state. SDS has not been confirmed in 7 counties in extreme southwestern Minnesota, although it may be present in some fields. This is a prime time for SDS symptoms to be showing up in soybean fields, and 2010 conditions, such as early planting and heavy and frequent rainfall in June and July, favor development of the disease. Other factors that favor disease development include compacted soil and poor drainage, high yield environments, high levels of soybean cyst nematode, and the planting of a susceptible variety (Note no varieties are completely resistant to SDS). Fields with a history of SDS are also likely candidates for a recurrence of the disease. Source: http://www.sleepyeyenews.com/news/x2023281479/Alert-for-Sudden-Death-Syndrome-in-Soybean

(Minnesota) **St. Paul courthouse open after suspicious substance found Monday.** The FBI is investigating a suspicious substance apparently mailed to the federal courts in St. Paul, Minnesota, and opened by an employee August 16. Authorities said a court worker opened some mail in the mailroom that afternoon, and noticed a short time later that the package had left a white, powdery residue on her hands. The U.S. Marshal's Service started evacuating the building and three court employees were taken to nearby Region's Hospital as a precaution. St. Paul police also responded to the incident, and the St. Paul Fire Department sent a hazardous materials team. Court officials said there was no immediate indication that the substance was dangerous, but the FBI said that it was investigating the incident and believed the substance came through the mail. Agents will be trying to trace the origin of the suspicious package. The courthouse was open August 17. Source: http://minnesota.publicradio.org/display/web/2010/08/17/courthouse-substance/

(Montana) **Evacuation ordered after prescribed burn flares on Stemple Pass.** Authorities ordered more than two dozen homes evacuated August 26 when a prescribed burn by Helena National Forest officials near the Continental Divide turned into an out-of-control wildfire, but a half-dozen Canyon Creek, Montana residents defied the order and stayed to protect their houses. Temperatures in the 90s and gusting winds caused the Davis Gulch fire to grow from 200 acres to between 1,500 and 2,000 acres in just a few hours, said an incident commander with the Montana Department of Natural Resources. More than 100 firefighters were trying to form an anchor behind the blaze and

protect the homes, but there was very little they could do to contain the fire. Residents in six of the 25 homes along the dirt and gravel road leading to Stemple Pass along the Continental Divide refused to leave their homes, said the Canyon Creek fire chief. The buildings were not in immediate danger of burning and firefighters were there to watch over the homes, he said. The prescribed burn was started August 25 to reduce fuel loads. Trees in the area have been killed by mountain pine beetles and spruce budworm. The National Weather Service had issued a fire weather watch the afternoon of August 24, and upgraded it to a red flag warning the afternoon of August 25 due to a forecast calling for high temperatures, high winds and low humidity. Residents questioned the wisdom of starting a fire in such conditions. But a Helena National Forest spokeswoman said U.S. Forest Service's burn plans are very specific and "they were within those specific prescriptions for this plan yesterday" when the fire was set. Source: http://missoulian.com/news/state-and-regional/article_bef02700-b15a-11df-81a0-001cc4c03286.html

(Montana) **Mandatory evacuation.** A mandatory evacuation order was in effect the morning of August 27, with 60 homes and structures threatened by a wildfire in the Bitterroot National Forest in Montana. The Downing Mountain Fire was first reported around 8 p.m. August 26. In a very short time it grew from 50 to 100 acres on private land, adjacent to the forest. The fire was sparked by lighting August 26. Sixty homes are in stage 2 evacuation, and an estimated 100 homes are in stage 1 warning of an evacuation. The area is 3 miles west of Hamilton. People living along Wyant Lane, Blodgett Camp Road, Canyon Creek Road, Grub Stake Road, and Owings Creek Road are all being evacuated. The Hamilton Fire Hall has been converted into an emergency operations center, and the Ravalli County Fairgrounds is open to evacuees needing assistance for pets and animals. The Red Cross has a team on site and is offering assistance. Source: http://www.nbcmontana.com/news/24782198/detail.html

(Montana) **Parts of county building to reopen after white powder scare.** Flathead County's Earl Bennett building in Kalispell, Montana was shut down August 12 after an envelope containing an unknown white powder was opened at the Department of Motor Vehicles (DMV). However, certain offices were scheduled to reopen August 13 at noon after authorities determined the powder did not pose a credible threat. According to the Flathead City-County Health Department, the building was still closed at 8 a.m. August 13. The building houses the county's DMV, treasurer, property tax, health department and planning and zoning offices. The health department and planning offices were scheduled to reopen at noon August 13, but the DMV, property tax and treasurer's offices will remain closed. The white powder fell out of the envelope just after 12:30 p.m. August 12. The building was evacuated and secured until the credibility of the threat could be evaluated. The powdery substance was sent to a Montana Department of Public Health and Human Services laboratory. Source: http://www.flatheadbeacon.com/articles/article/unknown_powdery_substance_shuts_down_flathead_county_building/19098/

National

(Louisiana) **Crews ready to kill well.**Contractors attached a new blowout preventer to an Assumption Parish, Louisiana oil and gas well and pumped in enough water August 26 to counteract pressure if the troubled well blows again, parish and oil company officials said. The 7,200-foot-deep Mantle Oil and Gas LLC well blew out August 11 and spewed oil, natural gas, brine, sand and other materials uncontrolled for nearly two weeks until it stopped on its own August 24, probably clogged with sand.

The old blowout preventer fell off a short time after the well went wild and fell to the side of the wellhead northwest of Paincourtville, according to Louisiana State Police reports. The blowout site, which was located in a large agricultural area west of Bayou Lafourche and north of La. 70, forced closures of La. 70 and La. 1003, and the evacuations of six homes, one business, and a race track. Source: http://www.2theadvocate.com/news/latest/101620048.html

(Missouri) **Nearly 6 tons of steel stolen from plant.** The Springfield, Missouri Police Department is investigating the theft of nearly 6 tons of stainless steel from the Southwest Wastewater Treatment Plant. The materials were used parts that were being stored in an outdoor area, according to police. The city will not need to replace the parts, which have an approximate value of $25,000. The materials include: 11 stainless steel hubs, 34 stainless steel blades, two stainless steel shafts and 480 stainless steel bolts. Parts began disappearing several weeks ago, but the bulk of the material appears to have been taken in recent days. Source: http://www.news-leader.com/article/20100821/NEWS01/8210342/Nearly-6-tons-of-steel-stolen-from-plant

Worldwide caution. The U.S. Department of State remains concerned about the continued threat of terrorist attacks, demonstrations, and other violent actions against U.S. citizens and interests overseas, and issued a precautionary travel advisory August 12. The State Department warned U.S. citizens that demonstrations and rioting can occur with little or no warning. Current information suggests that al-Qaida and affiliated organizations continue to plan terrorist attacks against U.S. interests in multiple regions, including Europe, Asia, Africa, and the Middle East, the agency noted. It said such attacks may employ a variety of tactics including suicide operations, assassinations, kidnappings, hijackings, and bombings. Extremists may also elect to use conventional or non-conventional weapons, and target both official and private interests, the State Department indicated. It cited several examples of such targets, including high-profile sporting events, residential areas, business offices, hotels, clubs, restaurants, places of worship, schools, public areas, and locales where U.S. citizens gather in large numbers, including during holidays. Source: http://travel.state.gov/travel/cis_pa_tw/pa/pa_4787.html

With oil well capped, scientists begin assessing spill's environmental toll. With the Deepwater Horizon well capped in the Gulf of Mexico, federal officials have turned their energies toward holding BP accountable for the environmental damage caused by hundreds of millions of gallons of oil loosed into the Gulf. An army of federal scientists 300 strong is focused on the area surrounding Mobile, Alabama. Hundreds of more scientists are at work in Mississippi and Louisiana. The goal is to create an official reckoning of the environmental toll, from the most obvious — 3,761 dead birds and counting, according to BP. Complicating the process, BP has an army, too, with scientists spread along the coastline from Texas to Florida hunting for the same answers that the government seeks. Both sides said that they hope to reach a consensus on what has been damaged, and what it will take to begin to restore the Gulf. The primary tool used to figure out what has been lost is the Natural Resources Damage Assessment. In essence, it amounts to a civil lawsuit, one that could take many years to settle. Source: http://blog.al.com/live/2010/08/with_oil_well_capped_scientist.html

INTERNATIONAL

Car bomb explodes outside Mexico TV studio. A car bomb exploded in the northern Mexican city of Ciudad Victoria August 27 outside a studio of top broadcaster Televisa, but there were no injuries,

Mexican media and witnesses said. Two witnesses saw the charred remains of a parked vehicle outside the TV studio in the city in Tamaulipas state, and Televisa's main morning news anchorman said nearby buildings were damaged, causing a power outage. No group was immediately blamed for the blast but drug cartels set off a car bomb in Mexico's most violent city Ciudad Juarez in July, the first of its kind, and another earlier this month in Tamaulipas in Mexico's escalating drug war. Source: http://www.publicbroadcasting.net/wxxi/news.newsmain/article/0/0/1693397/World/Car.bomb.explodes.outside.Mexico.TV.studio

Young girl among those hurt by acid in letters. An 8-year-old girl was among those injured by letters containing acid that were sent to the families of Geneva, Switzerland bank executives in recent days, the magistrate investigating the case said August 26. The girl was taken by ambulance to a hospital after she opened a box inside one of the letters and her hands were burned by concentrated sulfuric acid, the magistrate said by telephone from Geneva. Two adults were also injured, but apparently less seriously, by the letters, which targeted Geneva private bankers and their families, he said. The magistrate said that a total of eight letters containing acid were mailed to eight different addresses, in several cases the wives of executives at Geneva private banks. The letters were mailed from within Switzerland, but were routed through a central post office so it was not possible to say from where. The letters were sent August 22, the Swiss newspaper Tribune de Geneve reported. The motivation for sending the letters is not yet clear. Source: http://www.nytimes.com/2010/08/26/world/europe/26iht-swiss.html?partner=rss&emc=rss

Suicide bomber attacks Somali hotel, killing 32. A suicide bomber and gunmen wearing military uniforms attacked Muna Hotel near Somalia's presidential palace August 24, sparking a 1-hour gun battle with security forces. At least 32 people were killed, including six Somali parliamentarians. Witnesses described a horrific scene of dead bodies throughout the Muna Hotel and guests scrambling to safety by escaping out of windows. The multi-pronged assault came less than 24 hours after al-Shabab, a group allied with al-Qaida, threatened a "massive" war against what it labeled as invaders, a reference to the 6,000 African Union troops in Mogadishu. The attack on the Muna raised the 2-day toll to at least 70 people, a high number even by Mogadishu's violent standards. Fighting that rocked Mogadishu August 23 killed 40 people, health officials said. Somalia's deputy prime minister told The Associated Press that 19 civilians, six members of parliament, five security forces and two hotel workers were killed in the attack. Two attackers also were killed. Source: http://www.google.com/hostednews/ap/article/ALeqM5g7OaI4_kjeHA-o4UhlmP7vlWmrrwD9HPT6TG3

Disaster response experts call for 'red-helmet brigade'. As Pakistan struggles with the biggest natural disaster in its history, complaints are increasing over the slow international response and demands are growing for the creation of an international reaction force to cope with catastrophes. "When you look back at disaster after disaster, we are confronted with the same problems," said a Liberal MP from British Columbia. "The coordination of logistics on the ground always starts from square one. From the tsunami that hit Southeast Asia in 2004, to the earthquakes that killed thousands in Afghanistan and Pakistan, to the devastation Hurricane Katrina inflicted on the southern United States, to the Haiti earthquake, and now the floods in Pakistan, it is obvious we have learned very little." A medical doctor who has worked extensively on humanitarian crises in the developing world, the MP has long advocated having the United Nations establish a rapid response unit to

coordinate responses to natural disasters. Source: http://homelandsecuritynewswire.com/disaster-response-experts-call-red-helmet-brigade

Japan to inspect oil tanker after suspected Mideast attack. Officials for the United Arab Emirates have said they believe an explosives-laden boat struck the M Star in the July 28 "terrorist attack," which dented the hull of the Japanese vessel and slightly injured one crew member. Militant jihadists have made unconfirmed claims that a suicide bomber attacked the ship, owned by Mitsui OSK Lines and crewed by 16 Filipinos and 15 Indians, in the vital waterway leading to the oil-rich Persian Gulf. Japan has set up a special committee comprising self-defense force, coastguard, diplomatic, police and other officials, and the government has described the suspected attack as "extremely grave." The transport ministry has reported that the tanker's voyage data recorder captured radar images showing a small vessel making suspicious movements nearby around the time of the blast. The ministry also reported that the tanker suffered sizable damage both above and below the waterline, and that "extraneous material" had been recovered from the blast area, the official said. Source: http://news.ph.msn.com/business/article.aspx?cp-documentid=4292102

Flooding forces 250,000 to evacuate homes in China. Heavy rain over the last few days caused the Yalu River to breach its banks, rising to its highest level in a decade. Four people have died after their homes were swept away by flash floods. Flooding has also affected communities across the border in North Korea. Soldiers have been reinforcing rivers and using sandbags to protect against the high flood waters. The recent flooding is the latest disaster in the country's worst flooding season in over a decade. Source: http://www.wbko.com/news/headlines/101289979.html

China seized 100 tons of melamine-laced milk powder. China has seized more than 100 tons of melamine-contaminated milk powder in its northern provinces, state media reported late August 20, the latest case of food safety problems in the world's most populous country. A total of 103 tons of milk powder from four dairy brands in Hebei, Shanxi and Tianjin provinces were found to be laced with the industrial chemical melamine, the official Xinhua News Agency said. Authorities have detained 41 suspects. In July, samples of milk powder found in northwestern provinces Gansu and Qinghai had levels of the chemical melamine up to 500 times beyond the permitted limit. More than 124 tons of the milk powder in Qinghai have been seized since then, and six people have been arrested, Xinhua said. In 2008, melamine in Chinese milk powder, which caused the deaths of at least six children and made nearly 300,000 children ill, sparked global and national outrage. Melamine is an industrial chemical added to milk to fool inspectors by giving a misleadingly high protein level test reading. Source: http://www.reuters.com/article/idUSTOE67K00N

Eight Hong Kong tourists killed in Philippine bus hijacking. Philippine security forces stormed a bus packed with Hong Kong tourists August 23 to end a dramatic hostage crisis that unfolded live on global television, leaving eight people and the gunman dead. The day-long ordeal began when a disgruntled ex-policeman armed with an M-16 assault rifle and dressed in combat pants hijacked the bus in Manila's tourist district in a desperate bid to get his job back. Negotiations broke down after nightfall when the gunman, a former senior police inspector, began shooting and commandos were forced to storm the bus, firing dozens of bullets of their own into the vehicle. Police said a sniper shot the suspect dead after he used his captives as "human shields" in the final moments of the 12-hour standoff. Philippine's President said eight tourists were confirmed killed, while the Red Cross reported another seven were in hospital with unspecified injuries. Seven tourists, including children,

and two Filipinos were freed at various times throughout the day from the bus that was parked at Rizal Park, a popular tourist destination just a few blocks from police headquarters. The killings added to a fast-growing number of attacks of foreigners in the Philippines. Gunmen shot dead a South Korean man in a separate attack August 23 in another section of Manila. Police said the incidents were not related. Last month, an American, a South African, a Briton and their Filipina partners were killed in a spate of murder-robberies in Angeles City. The alleged killer was arrested. Source: http://news.yahoo.com/s/afp/20100823/wl_asia_afp/philippinescrimehijackhongkong

Garhi Khairo evacuated after breach in canal. Fresh breaches made in the Begari canal in Pakistan sent torrents of water gushing towards small towns and villages in Qamber-Shahdadkot district August 18, leading to forced evacuations of thousands. The water level in towns affected by earlier waves of floods was receding, but they were likely to remain inundated for several days. In Dadu, two artificial breaches of 50 feet were made in an embankment at Aghamani-Nau Goth and Aghamani-Nari road to protect three union councils of Mehar taluka, inundating 15 villages. The Indus was building up pressure along the Right Bank Outfall Drain-II, and two 100-foot breaches occurred in a valley near Laki Shah Saddar, inundating Shahnawaz Mallah, Bhatti, Chohan and Mahar villages. Villagers were trying to repair the town's protective embankment. Some parts of the Manjhand embankment were depressed or curved, and breaches were likely at these places. Stones were pitched and sandbags placed along the embankment, but the staff deployed at the embankment was insufficient to cope with an emergency. Source: http://www.dawn.com/wps/wcm/connect/dawn-content-library/dawn/the-newspaper/front-page/garhi-khairo-evacuated-after-breach-in-canal-980

Grenade thrown at Mexican TV station; no injuries. A grenade thrown by unknown attackers August 15 damaged apartments near a television station office in Monterrey, Mexico, but there were no reports of injuries, the country's state-run Notimex agency reported. The incident occurred at about 1:15 a.m. "Men in trucks" threw the device at the entrance to the television station. "The grenade exploded under a Toyota Tacoma pickup truck, which was badly damaged," according to Notimex. "It damaged a television live truck." Glass shattered in the apartment building, which was facing the entrance, Notimex said. Although employees were shaken up, no one was injured, the report said. Military patrols were not able to capture the grenade-throwers. Late August 14, a similar grenade attack occurred on the offices of Televisa in the city of Matamoros. A building was damaged but there were no reports of injuries. Source: http://edition.cnn.com/2010/WORLD/americas/08/15/mexico.station.grenade/#fbid=RvRBBEZyCwC&wom=true

4 of 61 missing ammo trucks found in MP. Four of the 61 trucks that vanished with 400 tons of explosives over four months were found – but thoroughly cleaned out – late August 13 in Northern India's Rajgarh district of Madhya Pradesh. A police team seized the vehicles parked in front of a local trading company, BM Traders, at Pipala village of Beoara Tehsil of Rajgarh district. The trucks were sent from Rajasthan Explosives and Chemicals Ltd (RECL) to a trading company in Sagar, Ganesh Magazine, between April and July. Following a Hindustan Times exclusive August 13, the Union Home Ministry expressed concern and asked the MP administration for a report on the missing trucks. The leader of the police team said the explosives were unloaded somewhere between Dholpur in Rajasthan and Sagar. While three of the seized trucks were from Bhilwara, the fourth one is owned by one of the two partners in Ganesh Magazine. Source: http://www.hindustantimes.com/4-of-61-missing-ammo-trucks-found-in-MP/Article1-586962.aspx

Russian wildfire area shrinks as storms knock out power for 96,000 people. Storms in northwest Russia knocked out power to about 96,000 people August 15, as emergency crews made headway in their battle against wildfires that have blackened 3,309 square miles this year. The storms in four regions, including the Leningrad region around St. Petersburg, packed winds as high as 67 mph, the emergency situations ministry said on its Web site. Almost 79,000 people still had no electricity at 6 a.m. August 16, and all customers should have power back by 8 p.m., the ministry said. The area of active fires in central Russia "significantly decreased" in the last 24 hours, the head of the ministry's crisis center said. Greenpeace Russia said there's hope things may change soon as rains and cooler temperatures are in the forecast. "It's still too early to relax," the environmental watchdog group said on its Web site. Source: http://www.bloomberg.com/news/2010-08-16/russian-wildfire-area-shrinks-by-14-as-storms-cut-power-to-79-000-people.html

Banking and Finance Industry

(Georgia) **Police: Sovereign citizen busted with $302 billion in fake bonds.** Investigators said a suspect tried to convince a Clayton County police officer that he did not have to follow any Georgia laws because he is a sovereign citizen. The officer pulled over the suspect's Chevy Avalanche in a traffic stop for speeding, but found he had no current tag, registration or insurance. A search of the truck found $108,000 hidden under the cup holders, police said. Then officers located several envelopes containing 12 fake surety bonds. "Basically, it's the U.S. government guaranteeing that this particular money is in the bank," said a police lieutenant who showed an investigative reporter one of the fraudulent documents allegedly worth $100 billion. The monetary total for all 12 fake bonds was $302.7 billion, police said. Investigators believe the suspect was planning to use the documents to attempt to steal houses, which was reported happening in neighboring counties in Georgia. Source: http://www.wsbtv.com/news/24764950/detail.html

Apple can't stop ongoing iTunes charge scam. Users of Apple's iTunes services should keep a close eye on PayPal and credit card statements for fraudulent iTunes charges. For more than a year, scammers have been racking up unauthorized charges on iTunes accounts, leaving Apple's customers to clean up the mess. Tech Crunch and the San Jose Mercury News report that the scam drains hundreds of dollars or more from accounts and that consumers have been complaining about the problem since at least early 2009. The number of people being hit by the fraudsters now seems to be growing, however. PayPal, which is often processing the unauthorized charges, confirmed August 23 that customers are being reimbursed for the fraud. The fraud "is happening on the iTunes side," a PayPal spokeswoman said via e-mail. She referred further questions about the scam to Apple. Scammers appear to be gaining access to the accounts by sending out fake phishing e-mail messages that try to trick users into disclosing their iTunes user names and passwords. Those credentials are then used to pile on charges for music or iTunes gift codes. Apple said that victims of the fraud must work things out with their banks and credit card companies. Source: http://www.computerworld.com/s/article/9181503/Apple_can_t_stop_ongoing_iTunes_charge_scam

U.S. military personnel targeted by malware. U.S. military personnel is again targeted by malware-peddling cybercriminals. Fake email purportedly coming from Bank of America is asking holders of Military Bank accounts to update them by following the given link. According to Trend Micro, the link

takes them to a very faithfully recreated bank login page, where they must enter their account username and password. So far, there is no indication that this is an actual phishing page, but the possibility exists. In any case, whatever information the victims enter, clicking on the "Sign In" button will take them to a page where an "Update Tool" is offered: The provided executable file is actually a ZeuS variant. But even if the victims choose not to download and install it because they became suspicious at the last moment, it may be already too late. The attack doesn't rely on manual download — it runs a multitude of browser exploits on the target systems as soon as the user lands on the page. Source: http://www.net-security.org/malware_news.php?id=1439

Last phase of credit card reform law in place, taking aim at penalty fees. The sweeping reform of the credit card industry was finally completed August 22 as the last pieces of the landmark federal law designed to stop unfair or deceptive practices took effect. The final phase restricts how much card issuers can charge in penalty fees compared with the amount of the violation. For example, if one is late paying a credit card bill with a $10 minimum payment, the penalty charge cannot be more than $10. In addition, new rules governing gift cards also took effect August 22 that require them to be honored for at least 5 years and allow only one fee per month. Congress passed the Credit CARD Act last year, which set up a rolling timetable to phase it in. The bulk of the law's provisions took effect in February, and prevented issuers from raising interest rates on existing balances, among other changes. The American Bankers Association, an industry trade group, called the implementation of the law a "transformative process that signifies a fundamental change for both consumers and the industry." A study by Pew Charitable Trusts released this summer showed that the largest card issuers have complied with the new regulations. However, Pew's study pointed out that the new rules do not limit increases in penalty interest rates, only the amount of fees. It also found that some credit card agreements did not disclose the size of any penalty rate hikes. The group has urged the Federal Reserve to issue rules governing those increases as well. Source: http://www.washingtonpost.com/wp-dyn/content/article/2010/08/23/AR2010082302260.html?hpid=topnews

(Oregon) **Bomb threat at Aloha, Oregon bank closes highway.** A bomb threat at a bank in Aloha, Oregon forced the closure of a busy highway for nearly two hours August 19, authorities said. Deputies of the Washington County Sheriff's Office responded to a 911 call from the bank located at 19091 SW Tualatin Valley Highway in Aloha at approximately 5.56 p.m. The highway is locally better known as TV Highway or Highway 8. "The caller made undisclosed demands and threatened to detonate a bomb in or near the bank if those demands were not met," said a police sergeant. "Sheriff's deputies quickly arrived on the scene and shut down SW TV Highway at SW 185th Avenue and SW 198th Avenue to protect motorists." The bank and some adjacent business were evacuated while the metropolitan explosives disposal unit looked for an explosive device, but they did not locate anything suspicious. Source: http://wireupdate.com/local/bomb-threat-at-aloha-oregon-bank-closes-highway/

Top phishing gang turns to Malware. An Internet security report released August 20 said phishing attacks dropped 10 percent from April to June 2010 year-over-year. While reassuring at first glance, the report states cybercriminals have shifted their schemes from old-school phishing e-mail attacks — which are designed to trick users into revealing personal information — to distributing Zeus malware, a more insidious form of cybercrime. Phishing attacks by Avalanche, one of the most prolific cybercriminal gangs (responsible for two-thirds of the world's phishing attacks in the second half of

2009), have disappeared, but other criminals have moved in to take its place, according to Internet Identity (IID). Phishing targets have shifted from banks to gaming, e-commerce and social networking sites, aiming to steal log-in information. However, Avalanche and others have turned to distributing Zeus malware which is capable of hijacking computers, then stealing banking, social networking and e-mail account logins, and making that information available as part of a criminal network. Once the malware has entered the user's computer, the identity theft is automatic — eliminating the need for the unsuspecting user to supply personal information in response to a fraudulent email. The U.S. continues to lead the world as the top hosting country for the origin of phishing scams. Canada moved from seventh to second in the report. Germany, U.K., France round out the top five. Russia and China are at the bottom of the list, according to the IID report. The sources for Zeus malware show a different worldwide distribution. Europe takes the top spot with 24 percent of malicious addresses, followed by China at 22 percent and the U.S. at 18 percent, reported Russian-based security software provider, Kaspersky Labs. Source: http://www.technewsdaily.com/top-phishing-gang-turns-to-malware-1071/

Credit card skimmers may be part of international scam. The rash of credit card fraud cases connected to skimmers on area gas pumps appears to be part of an international scam, according to the National Association of Convenience Stores (NACS) and the Alachua County Sheriff's Office (ACSO). Federal investigators said the scam is widespread in Florida — primarily along interstates — and has been found in other states. Florida has become a prime target for credit card skimmers at gas stations this summer in large part because of its ranking as third behind California and Texas in the number of convenience stores, according to the nation's largest convenience store trade organization. The Sunshine State is home to 9,223 convenience stores, and 7,280 of those stores — or almost 79 percent — have gas pumps, according to NACS, which represents 49 of the 50 top convenience store chains in the nation. An ACSO spokesman said one pattern investigators have noticed is that the card numbers are not used in the same area where they were stolen. Investigators in St. Johns County had documented about 200 victims so far this year, with most reporting card thefts during the summer months. The spokesman said he expects at least 200 victims to be identified in Alachua County this year. Source: http://www.gainesville.com/article/20100819/ARTICLES/100819347/-1/news?Title=Credit-card-skimmers-may-be-part-of-international-scam&tc=ar

Maine AG warns of credit card scam. Maine's attorney general is warning people to beware of an "advance fee" credit card scam that's targeting Maine residents. The attorney general said the scammers, who claim to be from "PeoplesChoice Savings," are offering a credit card with a $2,000 credit line. In exchange, they ask for $200 and the victim's bank account information so they can withdraw the funds. Officials with the PeoplesChoice Credit Union, which has several branches in southern Maine, said they have received several calls from consumers about the offer, which they emphasize they have nothing to do with. The attorney general said such advance fee credit card offers are fraudulent, and prey on people desperate for cash. She said consumers should never give out bank account or other personal identifying information over the phone or Internet without confirming the requestor's identity. Source: http://www.mpbn.net/Home/tabid/36/ctl/ViewItem/mid/3478/ItemId/13245/Default.aspx

(Michigan) **BBB warns of another advance fee loan scam.** The Better Business Bureau (BBB) has received several complaints over the last few weeks, from consumers across the country, inquiring

about a company identified as First National Financial Corp., allegedly located on Grand River Avenue in Brighton, Michigan. Consumers are informing BBB that they have been approved for a secured loan of $30,000 at a 7 percent interest rate with a required collateral deposit of $1,210, which is to be wired to Ontario, Canada. The Michigan Office of Financial & Insurance Services has informed BBB that First National Financial Corp. is not an active Michigan corporation and that it does not have a valid license to provide lending and financial services. The address is that of a former location for 1st Financial Lending, a legitimate Michigan firm located in Troy. 1st Financial Lending alerted the BBB to the use of their address and has no affiliation to the fraudulent operation. BBB's report on First National Financial is being revised to reflect the current investigation. Recent BBB investigations reveal an increase in bogus loan brokers who are impersonating legitimate lenders. They make illegal use of the names, logos and/or addresses of reputable financial institutions or organizations that have no affiliation or connection with the fraudulent operation. Source: http://tucsoncitizen.com/bbbconsumeralert/2010/08/16/bbb-warns-of-another-advance-fee-loan-scam/

Card skimmers found at Alberta mega-mall. A suspected bank-card skimming operation has been uncovered at the CrossIron Mills mega-mall near Balzac, north of Calgary, Canada police said August 20. Bank security experts alerted Royal Canadian Mounted Police (RCMP) commercial crime detectives after they found that two payment PIN pads at two retailers had been compromised. Mall officials said police advised them not to name the stores involved. The pads had been tampered with to capture financial data and gain access to accounts, said a RCMP constable. A full search of the 200 or so stores at the mall turned up two more skimming devices, investigators said. The transaction pads were likely installed in July. Some unauthorized withdrawals from bank accounts may have already occurred, but investigators think most of the potential fraud was interrupted. The culprits likely swiped the PIN pads while store clerks were not looking, substituting non-functional dummies while they added a wireless Bluetooth transmitter to the devices. Source: http://www.cbc.ca/canada/calgary/story/2010/08/13/calgary-balzac-crossiron-mills-skimming-pad-police.html

Credit card clearing house hacked says security researchers. An underground credit-card clearing house has been hacked, according to Trend Micro security researchers. Leaked data from the hack include employee e-mails and recorded phone calls. "A group of hackers recently published detailed information from an underground credit card company," writes an advanced threats researcher with Trend Micro. "On July 23, an anonymous group claimed to have compromised a server of an online credit card processor company. At that time, however, the extent of the compromise was unclear. Looking at the data that was published leads us to believe that the compromise is very plausible." Some of the stolen recorded conversations include individuals speaking about ways to defraud credit card companies. "This hacking incident would probably make a lot of cyber criminals nervous," the researcher writes. "Unfortunately, the incident also puts the personal data of legitimate customers and of many ordinary Russians at risk." Source: http://www.thenewnewinternet.com/2010/08/16/credit-card-clearing-house-hacked-says-security-researchers/

CHEMICAL AND HAZARDOUS MATERIALS SECTOR

(Massachusetts) **Authorities drill at MIT for 'Dirty Bomb' material theft.** Federal, state and local agencies August 19 responded to a simulated attempt by extremists to seize radioactive cobalt from the Massachusetts Institute of Technology (MIT) for use in a radiological "dirty bomb," the Boston Globe reported. The FBI and Energy Department coordinated the unpublicized exercise, which involved medical and fire personnel as well as state, city and campus police. The effort was part of the "Silent Thunder" series of drills, which focuses on responses by multiple levels of government to threats involving chemical, biological, radiological or nuclear weapons. Government sources refused to discuss difficulties that might have emerged in the drill, which addressed possible means of preventing would-be thieves from obtaining dirty-bomb ingredients as well as potential government responses to an attack involving radiological material or a different type of unconventional weapon. "Exercises of this type are valuable tools for enhancing coordination among the various organizations involved in response management," the MIT Nuclear Reactor Laboratory head said. Source: http://www.globalsecuritynewswire.org/gsn/nw_20100820_3693.php

(Missouri) **KC police arrest 14 protesters at site of plant that will make nuclear weapon parts.** Fourteen protesters were arrested August 16 at the construction site of a Kansas City, Missouri plant that will make parts for nuclear arms. The Kansas City Star reports the arrests came as about 75 people locked arms and marched onto the excavation site. The $685 million Honeywell plant is being built in southern Kansas City. Large earth-moving equipment was forced to stop operating during the march. Police used a loudspeaker to warn the protesters to disperse or face arrest. Most people walked back to the road, but the 14 who refused were charged with trespassing and taken to jail. Participants said they were there to protest America's continued proliferation of nuclear weapons. Source: http://www.kplr11.com/news/sns-ap-mo--protestersarrested,0,5244314.story

COMMERCIAL FACILITIES

(Florida) **Armed Christian militia pulls support for 'Burn a Quran' event.** An armed Christian organization which had pledged to protect a Florida church as it holds "International Burn a Quran Day" withdrew its support from the event August 25, according to a posting on its Web site. Right Wing Extreme also said in the posting it is asking the Dove World Outreach Center, based in Gainesville, Florida, not to hold the event, which is planned for the ninth anniversary of the September 11 terror attacks. The founder of Right Wing Extreme said since pledging its support and saying it would provide protection for the Dove Center, "we've all received several death threats" from the United States and beyond. The group has been in contact with the FBI, he said. He said he believes other groups may follow Right Wing Extreme and withdraw their support from the event as well. The pastor of the Dove World Outreach Center said the church will proceed with the event. He told CNN in an e-mail August 24: "We have met with the FBI who have warned us of the threats they have seen, not only against us but against other targets in Florida. We have personally received threats by phone and many by mail." Source: http://www.cnn.com/2010/US/08/25/florida.burn.quran.day/

(Florida) **Bomb scare shuts down polling place.** A suspicious package found near the Kiwanis Island Park Rec. Center in Merritt Island, Florida, August 24 closed a polling station. The bomb squad was called in to investigate. Brevard County elections officials said the ballots and voting equipment are secure. Voters who show up are being given a "pick-up" ballot and directed to the main elections office at 2575 North Courtenay Parkway. The Kiwanis Island polling place reopened once the bomb

squad gave the all-clear. Source: http://wdbo.com/localnews/2010/08/bomb-scare-shuts-down-polling.html

(New Hampshire) **Experts confirm device on Rye beach was pipe bomb.** Police August 19 confirmed the suspicious device found on Jenness Beach in Rye, New Hampshire was a pipe bomb that could have caused harm if ignited. The Rye police chief issued a statement saying his department had received information from the public and is continuing to work with state police and the FBI to locate the origin of the pipe bomb. The incendiary device, described as a silver pipe about 8-inches long, capped at each end, with a wick coming out of the side, was discovered along the water line around 6 p.m. August 14 by a beachgoer. Source: http://www.seacoastonline.com/apps/pbcs.dll/article?AID=/20100820/NEWS/8200373/-1/NEWSMAP

(Florida) **Report of gunman forces evacuation of Aventura office plaza.** Police have evacuated an Aventura, Florida office plaza after a woman told police she saw a man with a firearm inside the building. An Aventura police spokesman said they received a call from a doctor's office employee inside the plaza. The employee said a man came into the office asking questions when she noticed he had a firearm. The woman told police she got everyone out of her office, went to a nearby travel agency and called for help. Police arrived and evacuated the rest of the building. Source: http://www.miamiherald.com/2010/08/17/1780308/report-of-gunman-forces-evacuation.html

(Missouri) **Bomb squad called to Crestwood law office.** The bomb squad was called August 18 in Crestwood, Missouri, after an employee at a law firm spotted a suspicious device. When police arrived, they found a pipe, a cap and a fuse. Dozens of people were evacuated while police searched the area. However, the bomb squad detonated the device. Further investigation revealed no powder was found inside the pipe. Source: http://www.ksdk.com/news/local/story.aspx?storyid=212293&catid=3

(Florida) **Suspicious package prompts evacuation on Merritt Island.** An evacuation is under way at a Merritt Island shopping plaza as Brevard County Sheriff's agents in Florida investigate a suspicious package topped with a yellow bow, officials report. The suspicious package was reported about 1:35 p.m. August 13 near the Publix Supermarket at 1850 N. Courtenay Parkway. Deputies also cordoned off the area as sheriff's agents arrived to inspect the package. Surrounding stores were also being evacuated, officials reported. Source: http://www.floridatoday.com/article/20100813/BREAKINGNEWS/100813016/1006/NEWS01/Suspicious+package+prompts+evacuation+on+Merritt+Island

(New Hampshire) **Beach evacuated after apparent pipe bomb found.** A large portion of Jenness Beach in Rye, New Hampshire was evacuated August 14 while police disarmed what they believed to be a pipe bomb. Beach visitors saw a "metal pipe with two caps on either end that looked to be an explosive device," said the Rye police chief. The device was located along the water's edge during high tide. Rye police called in the New Hampshire State Police Explosive Disposal Unit, which disarmed the device using a "disrupter." The unit plans to test the device to determine if it was, in fact, a bomb or a hoax. It is unclear whether the device was placed along the water's edge or washed ashore, though "it looked as if it had been in the water for some time." Source: http://www.seacoastonline.com/articles/20100815-NEWS-8150319

Bomb hoax hits Lourdes pilgrims. Thousands of Roman Catholic pilgrims were evacuated from the Sanctuary of Lourdes in Lourdes, France after a bomb scare, which turned out to be a hoax. A Church spokesman told French news agency AFP that a telephoned warning had been received by police, announcing that four bombs were going to go off at around 2 p.m., August 15. The threat came as 30,000 worshipers gathered for the annual Feast of the Assumption, one of the pilgrimage site's busiest days of the year. Police gave the all-clear for the site to reopen after a search by bomb disposal teams with sniffer dogs. More than six million believers visit the Sanctuary each year. Source: http://www.bbc.co.uk/news/world-europe-10980157

(New York) **8 shot, 4 fatally, outside Buffalo, NY, restaurant.** Eight people were shot early August 14, four of them fatally, at a restaurant in downtown Buffalo, New York, police said. Managers had decided to close the City Grill in the city's business district after an altercation inside. The victims were leaving at about 2:30 a.m. when a man who had been inside began shooting, police said. A 25-year-old Buffalo man was charged August 14 with four counts of second-degree murder, but a prosecutor later told the Buffalo News that he intended to go to court August 15 to seek dismissal of the charges. "We need people to come forward," said a police commissioner, who estimated there were 100 people at the scene when police arrived. Source: http://www.google.com/hostednews/ap/article/ALeqM5igLvmLIYhe5ZTAtAcCkfnQZT8_HwD9HJNRO80

Communications Sector

Smartphones add to Wi-Fi data deluge. The demand for mobile connectivity is pushing the amount of data being sent over Wi-Fi networks ever higher, new figures from wireless network access firm WeFi reveal. Among the main findings of the WeFi Analytics Report Q2/2010: An Analysis of Global Wi-Fi, was a massive rise in the amount of data being sent to and from smartphones over Wi-Fi. The Android platform in particular saw tremendous growth, with 30 percent of Android platforms consuming 500MB to 2GB of data and 20 percent going over 2GB. Breaking down the figures for Android phones further reveals that 35 percent of devices monitored were in the United States, while the U.K. accounted for just 6 percent. Symbian devices are also gobbling up data, according to the report, with 32 percent of devices running the platform consuming between 100MB and 500MB per month, up from 20 percent in Q1, while 10 percent use over 2GB on Wi-Fi connections. Source: http://www.v3.co.uk/v3/news/2268801/wi-continues-grow-across-globe

(Missouri) **Thieves target telephone lines for valuable copper.** Copper thieves have been targeting the Springfield, Missouri area's lines of communication. "We've had several thefts recently where people have cut down our cables," said AT&T's regional director. Those AT&T lines were in northern Greene County, and were stolen from at least two different locations. The company said the lines cut were some main trunk lines that serve numerous customers. Also, at least 400 feet of Windstream's lines in southern Polk County were ripped off early August 20, leaving dozens of locals without a dial tone. Service to most customers was expected to be restored by Friday evening. Source: http://www.ky3.com/news/local/Thieves-targetting-telphone-lines-for-valuable-copper-101208594.html

(Missouri) **Phone outage in part of southwest Missouri's Polk County blamed on copper thieves.** Authorities in Polk County in a southwestern Missouri county said copper thieves were to blame for a loss of telephone service in some towns. KYTV reports that phone company crews worked August 20 to restore land-line service in the towns of Morrisville, Brighton and Pleasant Hope. Thieves had been cutting phone lines to sell the copper wire for several weeks in neighboring Greene County. Source: http://www.kplr11.com/news/sns-ap-mo--copperthieves-phones,0,6480317.story

BlackBerry emails can be monitored, says India. Indian officials may have come up with a way of monitoring encrypted corporate e-mails sent from BlackBerry devices, according to a government source. The method involves intercepting and making a copy of a corporate e-mail at the moment it is sent to a company's enterprise server, and then sending it on to the ISP's monitoring systems. "Enterprise mail services offered on BlackBerry platforms and other services provided on virtual private networks can possibly be monitored by feeding back a clear e-mail from the enterprise e-mail server to the monitoring system located at each of the ISPs' premises," said the Indian Department of Telecommunications, according to a report in the local Economic Times. It is still unclear whether the Indian authorities are looking to decrypt data, or would be happy with monitoring encrypted communications. Source: http://www.v3.co.uk/v3/news/2268476/rim-reaches-deal-bes-email

Trade groups oppose mandatory FM on mobile devices. Trade groups representing consumer electronics makers and mobile carriers have voiced opposition to a recent proposal by the radio and recording industries to require all mobile devices in the U.S. to include FM receivers. The proposal, made by the National Association of Broadcasters (NAB), comes as the trade group attempts to come to an agreement with a group affiliated with the Recording Industry Association of America (RIAA) in a longstanding battle over whether radio stations should pay royalties to record labels and performers for playing their songs. The NAB released the framework of a potential compromise over so-called performance royalties earlier this month: Radio stations would pay a royalty of 1 percent or less, and in exchange the U.S. Congress would require all mobile devices to include FM receiver chips. Source:
http://www.computerworld.com/s/article/9181018/Trade_groups_oppose_mandatory_FM_on_mobile_devices

Ferreting out rogue access points and wireless vulnerabilities. For almost 18 months starting in 2005, attackers used wireless networks at TJX and other retail chains to steal credit card data. The vulnerabilities were not an isolated instance: Subsequent research found that about half of all retail outlets in one shopping center had insecure wireless networks. Today, WiFi security has improved somewhat, but insecurities in installations still remain far too common. Vulnerability assessments of more than two dozen companies found a quarter have rogue wireless access points that were installed by employees, and a third of their wireless networks had misconfigurations that undermined their security, according to wireless security firm AirTight Networks, which conducted the tests. "A rogue AP is a very serious problem if you have it — an unmanaged, unknown device that is circumventing your defenses," said AirTight's CEO. "All the layers of defense that you worked so hard to put in can be circumvented by a single device that is communicating in the clear." Following the breaches at TJX and other retailers, the Payment Card Industry started requiring quarterly scans of wireless networks. It will likely increase the requirement to monthly scans. Firms that use wired-only scans are missing half of the picture, he said. Vulnerability scanning on the wired network could spot wireless routers, but it will not find insecurities in the network. Source:

http://www.darkreading.com/vulnerability_management/security/vulnerabilities/showArticle.jhtml?articleID=226700495&subSection=Vulnerabilities+and+threats

Mobile data offloading to double by 2015. The amount of mobile data being diverted from networks to ease congestion will triple to 48 percent over the next five years, according to a new report from ABI Research. Data traffic is expected to grow by a factor of 30 over the period, and recent figures from Ericsson suggest that mobile data is reaching monthly levels of 225,000 terabytes. Ericsson is tackling this by building new base stations, and recently announced its millionth, but ABI said that increasing capacity is not always an option. Traffic overload is starting to choke the mobile networks, and ABI recommended in its Mobile Network Offloading report that firms use new technologies to alleviate congestion. These should include Wi-Fi, femtocells, mobile content delivery networks and media optimization. ABI Research's practice director explained that by using these technologies, firms could save themselves from traffic overload. "Each of these offload and optimization technologies is aimed at solving a particular problem and they will all coexist. Wi-Fi is effective in covering limited areas containing many users, such as transport stations and sports venues," he said. By contrast, a femtocell would be a good option for targeting small numbers of heavy data users, while a mobile content distribution network could be used to cache files locally, lessening load, for example, should a video go viral. Compression, meanwhile, is the most popular method now and will continue to be so. Source: http://www.v3.co.uk/v3/news/2268286/mobile-saving-tech-triple

(Washington) **In Everett, Washington, the sabotaged towers of KRKO (1380) are being rebuilt.** The Snohomish News reports that work has begun on replacing two fallen towers in Everett, Washington, one a 349-foot tower and the other a 199-footer, in an effort to bring the station back to full power. The sabotaged towers of KRKO (1380) were literally pulled down, allegedly by an act of sabotage by ecoterrorists, last September. Radio-Info reported that two towers in the four-tower array were toppled by a group claiming to be from the Earth Liberation Front. KRKO has been running at reduced power. KRKO and its sports-talk format currently operates a nondirectional signal at 34,000-watts during the day and at 12,500-watts at night, and wants to increase their power output to 50,000-watts, but faces objections from area residents. Source: http://www.radio-info.com/news/everett-washingtons-sabotaged-krko-towers-are-being-rebuilt

CRITICAL MANUFACTURING

Mazda recalls 215,000 vehicles in U.S. for steering. Mazda Motor Corp has recalled 215,000 Mazda 3 and Mazda 5 vehicles sold in the United States because of the risk they could lose power steering without warning. The recall of vehicles from the 2007 through 2009 model years was announced in a filing with the U.S. National Highway Traffic Safety Administration (NHTSA) August 16. Mazda said the vehicles under recall could experience a "sudden loss" of power steering, increasing the risk of a crash. The notification did not detail any incidents. The defect occurs because rust could break loose from a high-pressure pipe, straining the power steering pump and causing the system to shut down, the Japanese automaker said. Mazda also said it was facing a shortage of parts to repair recalled vehicles at its dealerships. The automaker said it would begin to notify affected owners of the recall in September, and send notices to all owners by February. Source: http://www.reuters.com/article/idUSTRE67G5MM20100818?type=domesticNews

(Georgia) **Feds join copper theft investigation.** The U.S. Attorney General's Office in Atlanta and the FBI have joined the hunt to find three men accused of stealing $500,000 worth of copper from Southwire earlier this year. "Our office and the FBI are evaluating the case and will respond appropriately," said the first assistant U.S. Attorney, but added his office does not comment on pending investigations. A police lieutenant said the suspects have been linked to two similar cases in Florida, two in Georgia and one in Texas. The thefts in Georgia and Texas were also of copper, but the Florida incident was a theft of mixed metals that included copper. Southwire brokered the shipping of the stolen materials to Associated Trucking, which posted the job onto a trucking Web site. Associated Trucking was then contacted by a group of men claiming to be from LaRolle Trucking, a legitimate company based out of Miami/Hialeah, Florida. On April 29, three men made three trips into Southwire, each time loading 43,000 pounds of copper rods onto three tractor-trailer trucks, of which LaRolle has denied ownership. Southwire had arranged for the shipment to be sent to a destination in Indiana, but it never arrived. The incident was reported to police five days after it happened and the true identity of the suspects remains unknown. Source: http://www.times-georgian.com/view/full_story/9178001/article-Feds-join-copper-theft-investigation?instance=TG_home_story_offset

Tire tags reveal driver whereabouts. Researchers from Rutgers University and the University of South Carolina have found that wireless communications between new cars and their tires can be intercepted or even forged. While the potential for misuse may be minimal, this vulnerability points to a troubling lack of rigor with secure software development for new automobiles, said a co-lead on the study. The researchers presented their findings at the Usenix Security Symposium in Washington D.C. The system that the researchers tested monitors the air pressure of each tire on an automobile. The researchers had found that each sensor has a unique 32-bit ID and that communication between the radio frequency identification tag and the electronic control unit (ECU) was unencrypted, meaning it could be intercepted by third parties from as far away as 131 feet. An attacker could flood the control unit with low pressure readings that would repeatedly set off the warning light. An attacker could also send nonsensical messages to the control unit, confusing or possibly even breaking the unit. Component manufacturers could take some easy steps to strengthen the security of these systems, the researchers conclude. Communications could be encrypted. Also the ECU should filter incoming messages so that any with unexpected payloads should be discarded, so they do not corrupt the system. Source: http://www.businessweek.com/idg/2010-08-09/tire-tags-reveal-driver-whereabouts.html

Defense/ Industry Base Sector

F-22 lessons drive faster F-35 testing. Flight-testing of the F-35 Joint Strike Fighter at Edwards Air Force Base in California is running almost three times faster than expected, forcing program officials to accelerate follow-on support testing to keep pace. But program officials also confirm plans to add extra resources to tests to ensure the program stays on a revised schedule that extends development by 13 months. Since ferrying from Lockheed Martin's Fort Worth, Texas facility May 17, the two initial conventional-takeoff-and-landing (CTOL) F-35As have completed 53 sorties, 36 beyond the 17 they were slated to have finished by now. The commander of the Air Force Flight Test Center at Edwards said the F-35A is "exceeding expectations," and that the accelerated test rate is linked directly to aircraft performance and availability. As a result, tests of inlet rigs and weapons bay door opening will be conducted sooner than planned. The first two aircraft are focused on flight sciences objectives,

including envelope expansion, loads testing, flutter clearance and flying qualities. "Our objective by the end of 2010 is to clear the envelope to 40,000 ft. subsonic with 80 percent of the potential design limit load," the director said. In June, initial supersonic testing for loads and flutter was completed to Mach 1.2/580 KCAS and 39,000 ft. Air refueling clearance tests at 15,000 ft. are also getting underway. Source: http://www.aviationweek.com/aw/generic/story_generic.jsp?channel=awst&id=news/awst/2010/08/23/AW_08_23_2010_p31-249425.xml

Hydrogen-fueled UAV begins flight tests. Following an initial hour-long, battery-powered flight, AeroVironment's Global Observer unmanned aircraft is beginning a test program planned to culminate in a week-long flight in the stratosphere using liquid-hydrogen fuel. The flight debuts an innovative approach to persistent surveillance and marks a dramatic departure for a company that dominates the market for small, hand-launched UAVs. The Global Observer (GO) is flying from Edwards Air Force Base in Edwards, California where it will undergo an operational utility assessment under a Joint Concept Technology Demonstration sponsored by several U.S. agencies and led by Special Operations Command. The initial GO-1 aircraft is designed to stay aloft for seven days at up to 65,000 ft. carrying a 400-lb. payload. Source: http://www.aviationweek.com/aw/generic/story_generic.jsp?channel=awst&id=news/awst/2010/08/16/AW_08_16_2010_p42-246255.xml

Emergency Services

(Alabama) **Birmingham man arrested on terroristic threats charges.** The Birmingham Alabama Police Department (BPD) said they have arrested a man for making terrorist threats to an off-duty police officer. According to BPD, a 28-year-old man approached the officer while he was attending church and accused him of murdering his brother. The officer attempted to tell the suspect that he did not murder his brother, but the suspect continued to make threatening remarks to the officer. Birmingham investigators found the suspect to be referring to a 2001 shooting that involved the officer and the suspect's brother. The suspect's brother was a suspect in a robbery at the time and the officer was sent to investigate. According to the report, the victim opened the door and pointed a gun at the officer. The officer discharged his weapon and killed the suspect. An investigation into the shooting found it justifiable. Source: http://www.myfoxal.com/Global/story.asp?S=13010255

(Texas) **Texas gunman worked security, often praised police.** The man who killed himself during a shootout with a suburban Texas police department once worked as a jailer and security guard and even praised the very officers he attacked, according to associates and records. The man died of a self-inflicted gunshot wound to the head, the Collin County Medical Examiner's office said August 18. The announcement came a day after he towed a trailer loaded with explosives into the parking lot of the McKinney police station and set his pickup truck on fire, presumably to lure officers out of the building and shoot at them. He retreated to a field across a road and fired more than 100 rounds at police headquarters, the McKinney police chief said. The trailer did not ignite. Investigators found an assault rifle, a shotgun, and a handgun on him and later found more weapons in his home. Nobody else was injured in the attack in the suburb, about 30 miles north of Dallas. Police said they do not have a motive. According to the Texas Commission on Law Enforcement Officer Standards and Education, the suspect worked three months in 2001 at a federal prison operated by The GEO Group Inc. in San Antonio, but did not seek a permanent license when his temporary certification expired

after a year. Source: http://www.google.com/hostednews/ap/article/ALeqM5hjMxwz1U-4OVS-TsdxAMV5uqJChQD9HM64M00

(Texas) **Unexploded bomb found in trailer after police station shootout.** A gunman who opened fire the morning of August 17 at the McKinney, Texas Police Department evidently intended to detonate a bomb, authorities said. During a news conference August 17, police said the man's plan may have been to draw people out of the building and then to set off the explosive device. The McKinney police chief said the gunman parked his pickup truck and a trailer in front of the station August 17, and then set the truck on fire before retreating across a road and opening fire on the building. Source: http://www.kwtx.com/home/headlines/100888709.html

(Tennessee) **THP officer may have been target of early-morning bomb.** Police believe someone may be targeting a Tennessee Highway Patrol officer specializing in Driving Under the Influence arrests (DUIs) after a bomb went off at his home last month and two similar bombs exploded August 16 where he was working. A trooper was training two White House, Tennessee police officers on DUI detection at 1:30 a.m. when two bombs exploded on the west lawn of the police station, said a department of safety spokesman. Only the lawn was damaged. A third device was found later August 16 across the street in a neighbor's yard. A bomb disposal team for the Robertson County's Homeland Security District removed it. Homes in the area were evacuated, but residents began returning around 10 a.m. as police reduced the size of the protection area. Officials from the Tennessee Office of Homeland Security were at the scene.Source: http://www.tennessean.com/article/20100816/NEWS03/100816014/Bombs-explode-near-White-House-Police-Department

Energy

(Alabama) **Two people arrested for stealing copper in McCalla.** Two people have been arrested in connection with the theft of several hundred pounds of copper from an aerospace supply company in McCalla, Alabama. The Jefferson County Sheriff's Department said two men were arrested August 17 trying to sell the copper. Deputies said the men are suspects in two burglaries that happened at the company August 14 and 15. A detective, with the help of a local recycling company, caught the two men trying to sell the copper. The copper, described by deputies as "high-dollar copper Aerospace pins," was said to be worth more than $5,000. Source: http://www.myfoxal.com/Global/story.asp?S=13019798

(New York) **Vandals cause oil spill at RG&E's Russell Station property.** An environmental mess has been left in the area where vandals drained up to 4,800 gallons of oil from a spare transformer at an RG&E electric substation near Russell Station in Greece, New York. They did this so they could steal copper from inside the unit. The president of NYSEG and RG&E said, "We are doing all we can to expedite the containment and cleanup process. "We will be on the job until the cleanup is done." RG&E was notified of an oil sheen on Slater Creek adjacent to the Russell Station property August 16. The sheen was also visible on Lake Ontario, primarily to the east of Slater Creek. Right now, crews in Slater Creek are putting down foam pads to soak up oil. Based on the investigation of the oil spill thus far, RG&E believes the vast majority of oil is on or in the ground in the vicinity of the substation. The

incident was reported to the Greece police department. Source: http://www.whec.com/news/stories/s1702755.shtml

Food and Agriculture

(California) **Missouri dairy's raw milk cheese production stopped due to Listeria and Staph.** Inspectors with the Missouri Department of Agriculture have halted production and distribution from Morningland Dairy located in Mountain View, California, after raw cheese from the dairy tested positive for Listeria monocytogenes and Staphylococcus aureus. The cheese samples were seized June 30 in California; Missouri officials were made aware of the California department's test results today. Inspectors from the Missouri Department of Agriculture are coordinating with officials from the state department of health and senior services and the Food and Drug Administration to gather information concerning the distribution of the cheese from the dairy. The dairy sells several types of raw cows' milk and raw goats' milk cheeses across the United States. Source: http://www.foodpoisonjournal.com/2010/08/articles/food-poisoning-watch/missouri-dairys-raw-milk-cheese-production-stopped-due-to-listeria-and-staph/

(Iowa) **Salmonella strain blamed in outbreak is confirmed at 2 Iowa farms.** Laboratory tests have confirmed that two Iowa egg companies are contaminated with the same strain of salmonella blamed for a national outbreak of illness, which continues to claim victims and has sickened at least 1,500 people, federal officials said August 26. The confirmation backs up suspicions by the Food and Drug Administration (FDA) that tainted eggs from the two Iowa producers have caused the biggest case of Salmonella enteritidis disease that federal officials have seen since they began tracking the illness in the 1970s. The FDA, which has sent 20 investigators to the two farms — Wright County Egg and Hillandale Farms — said August 26 that it had detected the particular strain of salmonella in two barns at Wright County Egg, and in feed that the company made and gave to its own chickens. The agency also found that strain in feed that Wright supplied to Hillandale. "These are the very first results that we're beginning to get in, and there are many other results in the queue that may give us clues as to the the extent of contamination," the associate commissioner for food protection at the FDA said. He said the agency had taken 600 samples at the farms for laboratory analysis, and that additional results were expected. Officials from Wright County Egg said in a statement that the presence of salmonella on the property did not necessarily mean that the eggs were infected. But the company also pledged to work with the FDA. Source: http://www.washingtonpost.com/wp-dyn/content/article/2010/08/26/AR2010082604062.html

(Oregon) **Salmonella source identified at Umpqua Dairy.** Salmonella that contaminated packages at Umpqua Dairy's milk processing plant in Roseburg, Oregon, was found in equipment that washes and sanitizes crates receiving packaged milk and juice, the company's president said August 25. He said he did not know how the salmonella got into the system, which state health and agriculture officials say has been cleaned and now meets safety standards. “All the employees were working around the clock to make sure we sanitized that part of the company,” the president said at a press conference at the dairy. He said the company will continue to monitor the system. Officials have always thought the bacteria was on the packaging and not in the milk or juice, he said after the press conference. The Oregon Public Health Division attribute 23 cases of salmonellosis in nine counties to the bacteria at the dairy. Two people were hospitalized. The cases date back to October of last year. Health officials said that they only last week traced the illnesses to the dairy. The dairy shut down the Roseburg plant

last week, and voluntarily recalled products packaged there. Packaging resumed at the plant August 25, and milk and juice processed there will be in stores August 26. Source: http://www.nrtoday.com/article/20100826/NEWS/100829867/1063/NEWS&ParentProfile=1055

(New York) **Botulism fears bring herring recall.** Brooklyn's NY Fish Inc. August 23 recalled its NY Fish Brand (cold) Smoked Herring for being un-eviscerated prior to processing. The recall came after a routine inspection by the New York State Department of Agriculture and Markets Food Inspectors. No illnesses have been associated with the recall. NY Fish Inc. last year recalled smoked salmon and salted herring products for possible Listeria contamination, and a March 10, 2010 warning letter was sent to the company by the Food and Drug Administration (FDA) about conditions inside the seafood-processing facility. The latest recalled herring may be contaminated with Clostridium botulinum spores, which can cause Botulism, a serious and potentially fatal foodborne illness. This product was sold in New York. The recalled NY Fish Brand Smoked Herring comes in a coded, plastic vacuum bag with code number 141. Source: http://www.foodsafetynews.com/2010/08/botulism-fears-bring-herring-recall-1/

Nationwide meat recall announced. Zemco Industries in Buffalo, New York, has recalled approximately 380,000 pounds of deli meat that may be contaminated with bacteria that can cause a potentially fatal disease, the U.S. Department of Agriculture (USDA) announced August 23. The products were distributed to Wal-Marts nationwide, according to the USDA's Web site. The meats may be contaminated with Listeria monocytogenes, which was discovered in a retail sample collected by inspectors in Georgia. The USDA has received no reports of illnesses associated with the meats. The meats were produced on dates ranging from June 18 to July 2, 2010. The "Use By" dates range from August 20 to September 10, 2010. Source: http://www.cnn.com/2010/US/08/24/meat.recall/index.html?hpt=T2

(Texas; Oregon) **Pistachios Recalled for Salmonella.** Two companies recalled pistachios for potential Salmonella contamination last week. AustiNuts Wholesale, Inc., of Manor, Texas, recalled its pistachio kernel products and GloryBee Foods, Inc., of Eugene, Oregon, recalled its Aunt Patty's brand 5 pound bags of Whole Raw Pistachios and 25 pound boxes of Specialty Commodities brand Whole Raw Pistachios Kernels after the companies' supplier, California Delights, Inc., recalled 2 shipments of pistachio kernels for possible Salmonella contamination. According to a press release issued by AustiNuts Wholesale, the following products are being recalled because they contain the recalled pistachio kernels: Pistachio Kernels - Raw or Salted: Only lot numbers ending with "SE" with packing codes of P1860 through P2080 (Lot numbers must end in "SE"); Deluxe Nut Mix, Salted:Only lot number P187013201AW through P207013201AW (Lot numbers must fall between P1870 and P2070); -Gourmet Nut Mix, Salted: Only lot number P195014401AW through P201014401AW (Lot numbers must fall between P1950 and P2010). Source: http://www.foodsafetynews.com/2010/08/pistachios-recalled-for-salmonella/

Half a billion eggs have been recalled. The number of eggs recalled in a nationwide salmonella scare has grown to more than half a billion. Iowa egg producer Hillandale Farms of Iowa is voluntarily recalling some 170.4 million eggs distributed to stores and companies that service, or are located in, 14 states, a spokeswoman at the Egg Safety Center said August 20. The Hillandale eggs were distributed under the Hillandale Farms, Sunny Farms, and Sunny Meadow brand names in six-egg cartons, dozen-egg cartons, 18-egg cartons, 30-egg packages, and five-dozen-egg cases, the Web site

for the Egg Safety Center said. Loose eggs, which could be repackaged by customers, were packaged under the Wholesome Farms and West Creek brands in 15- and 30-dozen tray packs, according to the Egg Safety Center. The salmonella outbreak prompted Wright County Egg of Galt, Iowa, which began recalling eggs last week, to increase its recall to 380 million eggs August 18. The number of salmonella cases is expected to grow because infections after July 17 may not have been reported yet due to a two- to three-week lag between when a person becomes sick and when the case gets reported in the system, the Centers for Disease Control and Prevention (CDC) said. Source: http://edition.cnn.com/2010/HEALTH/08/20/eggs.recall.salmonella/?hpt=Sbin#fbid=RvRBBEZyCwC&wom=false

(California) **82-square-mile quarantine declared for melon fruit fly.** Six melon fruit flies were caught in traps the week of August 9 near Mettler, California, about 25 miles south of Bakersfield. The flies have the potential to devastate Kern County's agriculture industry. "I think every farmer's probably concerned about it, and I think they'd be lying if they weren't," a local farmer said about the flies. The problem with the fly is that it lays its eggs in fruit, making it inedible. Because five flies were found in a single trap, an 82-square mile quarantine is now in effect. The earliest it could be lifted is April 2011. "An insect of this magnitude could potentially devastate not only Kern County, but the whole state's $45 billion industry," Kern County's agricultural commissioner said. The flies were found near a pepper field northwest of Mettler. Since August 16, crews from the California Conservation Corps and the California Department of Food and Agriculture are working to remove every single pepper from the field. Source: http://www.bakersfieldnow.com/news/local/101127014.html

Salmonella recall expands to eggs sent to 17 states. The Iowa producer of shell eggs linked to hundreds of illnesses in a massive salmonella outbreak has expanded its recall to include eggs sent to 17 states, federal health officials said August 19. Wright County Egg of Galt, Iowa, now said the potentially tainted eggs were distributed to wholesalers, distribution centers and food service companies in California, Arizona, Missouri, Minnesota, Texas, Georgia, Washington, Oregon, Colorado, Nevada, Iowa, Illinois, Utah, Nebraska, Arkansas, Wisconsin and Oklahoma. At least 380 million eggs have been implicated in the outbreak, which is confirmed to have sickened people in four states and is suspected in several more. The Centers for Disease Control and Prevention is working with state health departments to investigate the illnesses. No deaths have been reported. Source: http://www.msnbc.msn.com/id/38741401/ns/health-food_safety?Gt1=43001

Tainted poultry litter causing widespread arsenic contamination. The U.S. Department of Agriculture's Agricultural Research Service has pinpointed a major source of arsenic contamination in the environment — poultry litter. Commercial poultry producers often supplement chicken feed with roxarsone, an arsenic-based food additive, in order to bulk them up and prevent parasites from forming in their systems. But this toxin ends up contaminating local water supplies and crop fields. Roxarsone helps to prevent commercial chickens from becoming infected with parasites, and it also helps to promote weight gain, but the birds end up excreting it into their litter. This litter is then spread on crop fields where it poisons not only the soil, but also nearby rivers and streams. Natural chicken litter is full of nutrients and is beneficial to crop soil, but when full of arsenic, it is poisonous and toxic to the environment. Defendants of roxarsone insist that the additive is safe because it is derived from organic arsenic, but studies have shown that organic arsenic converts to the harmful, inorganic kind when it reacts with the bacteria in chicken manure. Source: http://www.naturalnews.com/029517_poultry_arsenic.html

(Nevada) **30 cases of Salmonella in the valley linked to eggs and poultry.** The Southern Nevada Health District has reported 30 cases of Salmonella since January of 2010. All are linked to a string of bacteria that's typically associated with eggs and poultry. While experts say this is by no means an outbreak, they do want to let people know that avoiding contamination boils down to cleanliness and common sense. In the last 8 months the number of residents that have become infected with Salmonella Enteritidis, has nearly quadrupled in Clark County. The illness can be more severe among the elderly and children. Source: http://www.ktnv.com/Global/story.asp?S=13000210

Tropical fruit cited in US typhoid fever outbreak. Federal and state health agencies said frozen mamey fruit pulp is the probable cause of seven confirmed and two suspected cases of typhoid fever (Salmonella Typhi infections) in California and Nevada. The Centers for Disease Control and Prevention (CDC) announced the outbreak August 12 and said epidemiologic evidence points to mamey fruit pulp produced by Goya Foods, Inc. of Secaucus, New Jersey. The company recalled 14-ounce packages of the tropical fruit product August 11. Typhoid fever is common in the developing world, but only about 400 cases occur in the United States annually, with about 75 percent of them in international travelers, according to the CDC. The infection causes high and sustained fever, headache, constipation, malaise, chills, and myalgia, and it can be severe or fatal if not treated. It typically spreads through contaminated food or water. In its recall announcement, Goya said the mamey fruit pulp comes in 14-ounce plastic packages that are not marked with a lot number or expiration date. The UPC number is 041331090803. The product is distributed in retail stores in Alaska, Arizona, California, Colorado, Hawaii, New Mexico, Nevada, Oregon, Texas, Utah, and Washington. Source: http://www.cidrap.umn.edu/cidrap/content/fs/food-disease/news/aug1310typhoid.html

Government Sector (including Schools and Universities)

Network security challenges faced by universities. Striking a balance between an open yet secure network remains a challenge for university IT departments. While universities are often on the cutting edge of innovation, they face complications when it comes to enforcing IT policies. In some cases, this has led to staggering data breaches. For example, last year, the University of California at Berkeley faced a difficult situation when overseas hackers gained access to data on tens of thousands of people who have received healthcare from the university. The victims' medical information and Social Security numbers were exposed in the breach that lasted from October 2008 to April 2009. The University of Florida faced a similar breach last year. While security protocols, like requiring two-factor authentication for network access, could prevent breaches, enforcement and implementation challenges abound. While it is unrealistic and unwarranted for universities to be held to the same standard as the enterprise, there are best practices schools can incorporate to strengthen their security. Source: http://www.net-security.org/article.php?id=1481

New SWAT tactics for school shootings. A full-scale exercise at a high school in Utah focused on the latest police and SWAT tactics for Columbine-style school shootings and intruder attacks. The federal training for school staff allows schools to partner up with local first responders and improve school safety. New technologies turn basic school radios and surveillance cameras into tools that help police and SWAT teams achieve the pinpoint accuracy of a smart bomb when it comes time to neutralize

violent offenders. A video of the exercise was produced using only the unrehearsed radio dialog captured during the exercise and the synchronized video footage caught on eight different surveillance cameras mounted outside and in the school hallways. As one follows the shooters, one notices exercise facilitators operating the smoke machine and dispensing ammo to the perps as they take hostages. The maneuvers of the three law enforcement teams in the video are based on the information they receive moment-by-moment, with no scripting. The school principal also provides crucial behind-the-scenes support so teams can quickly box in the gunmen before rushing through the last door to take them down. Source: http://www.schoolsafetypartners.org/communications/679-New-SWAT-tactics-for-school-shootings.html

(California) **Copper theft causes blackout at UCSF Medical Center.** The University of California, San Francisco Medical Center at Mount Zion ran on backup generators for the majority of August 25 after thieves stole a copper ring from a transformer causing the main power generator to fail. According to a PG&E spokesman, the outage was isolated to the hospital, and crews on scene determined a copper ring essential to transferring power was stolen from the transformer. PG&E remains at the location to determine if the problem can be immediately fixed or if the utility company will have to bring in additional generators to supply the hospital with power. Source: http://www.sfexaminer.com/local/Copper-theft-causes-blackout-at-UCSF-Medical-Center-101577753.html

(Texas) **McKinney police building's success against gun attack shows value of secure design.** After not one employee felt a scratch when a suspect fired more than 100 rounds at the McKinney, Texas public safety building August 17, the building itself became a hero. Praised in public by the mayor and police chief, the bulletproof fortress represents the new breed of municipal buildings. In an era of homeland security, even the smallest towns are erecting safeguarded structures designed to keep people out rather than draw them in. And on August 17, it paid off. "We saw the design change after the Oklahoma City bombing," said a man whose company, Pogue Construction, led the $17.6 million McKinney project four years ago. "Whereas before people thought of public buildings as open spaces to see your tax dollars at work, now they've started thinking about those people's safety and closing off the building. The intent is to separate." Secure access points and the arrangement of rooms create a buffer between McKinney law enforcement officials and the public. Windows sit just above eye level to prevent direct attack. They slope to limit ledges for explosive devices. Bulletproof glass protects the lobby, and bullet-resistant liner lies inside the masonry walls. Source: http://www.dallasnews.com/sharedcontent/dws/news/city/collin/mckinney/stories/082210dnmetmcshooting.258565a.html

(Arizona) **Bomb threat closes a Peoria high school.** Peoria, Arizona police are investigating a bomb threat at Centennial High School, which has caused the evacuation of the school. A Peoria police spokesman said about 900 students were cleared from the school after a phoned-in bomb threat to the school around 9 a.m. August 19. The police spokesman said the evacuated students were taken to two nearby churches and another nearby high school. He said the campus was searched and no device was located. There were 40 evacuees who were evaluated by fire paramedics for heat injuries, and paramedics treated 12 of them on scene and took 3 to hospitals with heat-related issues, the spokesman said. The students were sent home by district officials and school was canceled for the day. Source: http://www.kpho.com/news/24703185/detail.html

Obama orders uniform access to classified info. The White House this week ordered the Secretary of Homeland Security to issue guidance for the uniform handling of classified information shared by the federal government to state and local governments. In an executive order delivered August 18, the President tasked DHS with producing those procedures within 180 days after consulting with other top agencies, and the director of national intelligence. Once established, the DHS security secretary will continue to serve as executive agent for the classified information program, the order said. The order applies to state, local, tribal, and private sector entities that receive federal classified information. Those entities must handle that information under procedures stipulated in a number of executive orders dating back to 1993. The rules to be issued by DHS will ensure uniformity in following those orders. Designated individuals in state, local, tribal, and private sector entities may receive classified information under the order once they are determined eligibly by a sponsoring federal agency, the order noted. Applicants must demonstrate a need for access to top secret, special access, or sensitive compartmented information. Clearances granted to all individuals representing such entities will receive reciprocity from other federal agencies, the order said. The organizations must properly protect any classified information they receive. Source: http://www.hstoday.us/content/view/14425/128/

National Guard Bureau tells what not to write on Facebook. The National Guard Bureau is giving guard members specific guidance on how to control their privacy settings on Facebook, and what to avoid publishing on social media sites. The guidance advises guard members to use "friends only" privacy settings on social networking sites. It also warns that members' social network "friends" and "followers" could be factors in background investigations when the members apply for security clearances. "Remember, what happens online is available to everyone, everywhere," wrote the bureau's public affairs director, in an August 16 news release about the policy. "There should be no assumption of privacy when guard members begin to interact with others online." The guidance prohibits members from publishing any content distributed internally by the guard that has not been officially approved for release to the public. The policy bans publishing internal "memos, e-mails, meeting notes, message traffic, white papers, public affairs guidance, pre-decisional materials, investigatory information and proprietary information" if those materials are not specifically authorized for release, according to the news release. Source: http://fcw.com/articles/2010/08/20/national-guard-bureau-gives-advice-on-what-not-to-write-on-facebook.aspx

Pentagon takes aim at China cyber threat. The U.S. for the first time is publicly warning about the Chinese military's use of civilian computer experts in clandestine cyber attacks aimed at American companies and government agencies. In a move that is being seen as a pointed signal to Beijing, the Pentagon laid out its concerns this week in a carefully worded report. The People's Liberation Army, the Pentagon said, is using "information warfare units" to develop viruses to attack enemy computer systems and networks, and those units include civilian computer professionals. The assertion shines a light on a quandary that has troubled American authorities for some time: How does the U.S. deal with cyber espionage emanating from China and almost certainly directed by the government — despite the fact that U.S. officials don't have or can't show proof of those ties? Asked about the civilian hackers, a Defense Department spokesman said the Pentagon is concerned about any potential threat to its computer networks. The Pentagon, said a spokesman will monitor the PLA's buildup of its cyberwarfare capabilities, and "will continue to develop capabilities to counter any

potential threat." Source: http://www.google.com/hostednews/ap/article/ALeqM5i49n7xcjIHBv_Uq9SOjyP7vs6f8wD9HMP8R00

(Texas) **Fort Hood gate briefly closed after explosive trace found.** Officials in Fort Hood, Texas, temporarily closed the East Range Road gate early August 19 after gate guards discovered a cement truck with possible traces of explosive residue during a routine vehicle search. The guards immediately alerted Fort Hood Emergency Services who set up a full security perimeter around the vehicle in question. All traffic was redirected to other gates while further tests were conducted. These tests indicated that the vehicle did not contain any explosives, and the gate was reopened to all vehicular traffic. Source: http://www.statesman.com/blogs/content/shared-gen/blogs/austin/blotter/entries/2010/08/19/fort_hood_gate_briefly_closed.html?cxntfid=blogs_the_blotter

(Connecticut) **Laptop with Social Security numbers stolen from UConn West Hartford.** University of Connecticut officials are investigating the theft of a laptop computer from its West Hartford campus that contains the names and Social Security numbers of 10,174 applicants, many of whom were selected for consideration to attend the regional campus. This is the second incident of a missing laptop with sensitive information made public this week. The state attorney general is investigating the theft of a laptop from the Yale School of Medicine that contained clinical health information for approximately 1,000 patients. UConn officials said the theft of its laptop, which was being kept in a storage cabinet at the West Hartford campus information technology department, was discovered August 3. They said steps have been taken to prevent unauthorized access to the university through this computer, and there is no indication it was stolen for the purpose of identify theft. Source: http://www.westhartfordnews.com/articles/2010/08/19/news/doc4c6d6ca4879e4991899745.txt

Alaska couple compiled hit list with 20 names, say feds. A rural Alaska couple compiled a hit list of 20 targets, including members of the military and media, and had moved to the operational phase of their plan, according to documents filed in federal court August 16. The couple, who hail from King Salmon, Alaska, have pleaded guilty to lying about the list and making false statements to the FBI in May. Under a plea agreement, the husband will serve eight years in prison and three years probation while his pregnant wife will serve probation. Sentencing is scheduled August 23 in U.S. District Court in Anchorage. The husband's public defender claims her client was lonely in King Salmon and befriended an undercover Alaska State Trooper while attending mosque during trips to Anchorage. Prosecutors alleged that the husband, also known as "Bilal," converted to Islam about a decade ago, and began studying the teachings of an American-born cleric who has professed hatred for the United States and who supports acts of terrorism. Source: http://www.cbsnews.com/8301-504083_162-20014076-504083.html

(New Mexico) **Virus infects Sec. of State's computer.** Questions are being raised after some New Mexico state employees, including the office manager said they saw computer viruses display pornographic icons on the New Mexico secretary of state's laptop computer. Answers have been hard to come by because the former IT director has left the country and both the deputy and the secretary herself insist the virus was not pornographic, but it is clear there were some serious security issues. The office administrator said he was concerned about computer security given that the office keeps thousands of social security numbers and secret addresses of domestic violence

victims who have their identities protected. “It could have had the potential even to have that information leaked to the public where people’s safety could have been compromised,” he said. The administrator recorded undercover video of the IT staff trying to get rid of powerful viruses that had infected the official’s state laptop. A staff member can be overheard saying he sees 158 viruses on the computer. The main virus appears to be one called the Defense Center which disguises itself as anti-virus software and takes control of a computer and forces pornographic links on the desktop. Source: http://www.kob.com/article/stories/S1699185.shtml?cat=517

Employees still pose biggest security threat, survey finds. Workers inside agencies pose the biggest threat to computer security; provide foreign governments and other perpetrators direct access to sensitive networks, according to results of a survey of security experts released August 17. Most of the 22 government security experts security vendor PacketMotion surveyed pointed to employees as the greatest threat to steal sensitive information because of failure to comply with policies combined with lax controls often provide easy access to data. Results of the survey reflect “the reality that the [perpetrator] will hijack or use the credentials of internal users,” said the vice president of marketing and product strateat PacketMotion. The survey was conducted during the Black Hat USA 2010 conference in Las Vegas in July. Fifty-nine percent of those surveyed said employees represent the biggest threat to the government’s enterprise computing environment, 14 percent pointed to administrators who have been given access to certain networks and files as threats as well. Eighteen percent said outsiders, including contractors, were the biggest security threat, while only 9 percent named hackers and cyber criminals the top threats. Source: http://www.nextgov.com/nextgov/ng_20100817_1347.php

Hacked smartphones pose military threat. Hacked smartphones could endanger troops by sending location data to the enemy using mechanisms similar to those employed by recently discovered Android malware, experts said. Malicious software that commandeers phone functions could give wartime enemies valuable information about troop locations and movements, according to a software security professor at Columbia University and conference chairman for the RSA Confernece, and an analyst who works on the PayPal online security and malware strategy team.”Even normal apps can send a lot of information back home,” the professor said, and individual users are generally ill equipped to determine whether these apps represent security risks. The analyst said he has discussed the problem with the Defense Advanced Research Projects Agency (DARPA). In fact, DARPA brought it up. “I would say the military are aware of it but not very comfortable with it,” he said. Source: http://www.computerworld.com/s/article/9180768/Hacked_smartphones_pose_military_threat

Most attacks on federal networks financially motivated. Most malware attacks against federal agencies are financially motivated, seeking to trick computer users into buying fake security software or providing personal information that can be used to hack into their bank accounts. Although espionage and terrorism often are considered the primary motivations for breaking into government networks, 90 percent of incidents of malware detected on federal computers in the first half of 2010 were designed to steal money from users, according to data collected from the U.S. Computer Emergency Readiness Team at the Homeland Security Department. “This statistic represents the dominance of financially motivated malware within the threat picture,” said the section chief of the surface analysis group at US-CERT. “It is not that the federal government is being targeted by

organized criminals; it is that we are a smaller portion of a larger global community impacted by this." Federal officials must consider equally the targeted threat, which the section chief equates to a sniper attack, and the widespread or "battalion" attack. Source: http://www.nextgov.com/nextgov/ng_20100813_1419.php

Information Technology and Telecommunications

Rootkit with Blue Screen history now targets 64-bit Windows. A new version of malware that crippled Windows PCs last February sidesteps safeguards designed to block rootkits from hijacking machines running 64-bit editions of Windows, researchers said August 26. "A new era has officially dawned; the era of x64 rootkits," said a Prevx researcher in a post to the company's blog. The updated rootkit, which goes by names including Alureon, TDL and Tidserv, is able to infect 64-bit Windows PCs. Both Prevx and Symantec have found evidence that hackers are actively using the rootkit. "The infection is spreading on the Web, by using both porn Web sites and exploit kits," he said, adding that U.K.-based Prevx spotted the new rootkit more than 1 week ago. Symantec's first sighting was August 25. The new rootkit sidesteps two, important anti-rootkit protections Microsoft built into 64-bit Windows, Kernel Mode Code Signing and Kernel Patch Protection, also known as PatchGuard. The pair are designed to make it more difficult for malware to tamper with the operating system's kernel. Rootkits that overwrite the hard drive's master boot record, where code is stored to bootstrap the operating system after the computer's BIOS does its start-up checks, are essentially invisible to the operating system and security software. Source: http://www.computerworld.com/s/article/9182238/Rootkit_with_Blue_Screen_history_now_targets_64_bit_Windows

Blogger identifies privacy flaw in Facebook Places, as Foursquare co-founder calls the tool 'boring'. The Facebook Places application has been accused of falling short when it comes to protecting its user's locational privacy. A information security blogger and assistant professor at the school of information studies at the University of Wisconsin claimed Facebook Places falls short on privacy as non-authorized check-ins by friends are visible. He said Facebook has tried to do a better job addressing privacy with Places compared to some previous launches of new "features." However, he noted that as he has played around with the service, he claimed to have uncovered a problem with Facebook's assertion that "no one can be checked in to a location without their explicit permission." He said: "While Places is largely an opt-in service — one needs to install and use it on a mobile device — anyone can be 'checked-in' to any place by a friend. This can happen regardless of whether you use the service yourself. If you get checked into a place by someone, and you haven't already authorized the service or these kinds of check-ins, you'll receive an e-mail asking if you want to allow check-ins by friends." He said that his wife had been "checked in" despite not authorizing use of the feature. If any of his friends looks at his Facebook feed, they will see the status update of his check-in at the store, with his wife's name there. Her name also appears with his check-in on the location's page, which is automatically generated by the places service. Source: http://www.scmagazineuk.com/blogger-identifies-privacy-flaw-in-facebook-places-as-foursquare-co-founder-calls-the-tool-boring/article/177307/

Anti-virus products struggle against exploits. Most anti-virus products designed for use in businesses do a poor job of detecting exploits that hacked and malicious Web use to foist malware, a new report concludes. Independent testing firm NSS Labs looked at the performance of 10 commercial anti-virus

products to see how well they detected 123 client-side exploits, those typically used to attack vulnerabilities in Web browsers including Internet Explorer and Firefox, as well as common desktop applications, such as Adobe Flash, Reader, and Apple QuickTime. Roughly half of the exploits tested were exact copies of the first exploit code to be made public against the vulnerability. NSS also tested detection for an equal number of exploit variants, those which exploit the same vulnerability but use slightly different entry points in the targeted system's memory. None of the exploits used evasion techniques commonly employed by real-life exploits to disguise themselves or hide from intrusion detection systems. Among all 10 products, NSS found that the average detection rate against original exploits was 76 percent, and that only 3 out of 10 products stopped all of the original exploits. The average detection against exploits variants was even lower, at 58 percent, NSS found. Source: http://krebsonsecurity.com/2010/08/anti-virus-products-struggle-against-exploits/

Chrome, Safari see surge in vulnerabilities. Web application vulnerabilities during the first two quarters of 2010 represent a smaller percentage (66 percent) of total commercial application vulnerabilities (4,019) than they did during the latter two quarters of 2009 (82 percent of 2652). But Web application vulnerabilities during the first half of the year (2,645) were about the same as the total number of vulnerabilities in commercial apps detected during the second half of 2009, while the overall number of application vulnerabilities in 2010 increased by 50 percent. As noted in the Cenzic Q1,Q2 2010 Trends Report, some 60 percent of these Web vulnerabilities still have no fix available and exploit code is publicly available for about 45 percent of them. Comparing the Q1/Q2 2010 period to the Q3/Q4 2009 period, the report observes that while Mozilla Firefox and Microsoft Internet Explorer had fewer vulnerabilities (59 vs. 77 and 40 vs. 44, respectively), Apple Safari and Google Chrome exhibited far more vulnerabilities (83 vs. 25 and 69 vs. 25). Nonetheless, all browser makers have addressed vulnerabilities promptly, Cenzic says. Cenzic attributes the soaring number of vulnerabilities in Safari and Chrome toWebKit, the open-source rendering engine used in both browsers, and to iPhone and Android flaws. Source: http://www.informationweek.com/news/storage/security/showArticle.jhtml?articleID=226700519

Rogue AV uses legitimate uninstallers to cripple computers. The fact that some rogue AV solutions try to prevent the real ones from doing their job is widely known in the security community, but CoreGuard Antivirus — a "popular" fake AV solution - has been spotted utilizing legitimate software uninstallers to trick users into uninstalling their legitimate security software. When the malicious file is executed, a message box opens up. Clicking on the "OK" button — or even on the "Close" button — starts the installer of the antivirus in question. Symantec researchers reveal that the fake solution searches for uninstaller information in the Windows registry and launches the right uninstaller for certain legitimate AV solution installed on the system, such as products from Microsoft, AVG, Symantec, Spyware Doctor, and Zone Labs. It then tries to download "AnVi Antivirus," another rogue AV that is actually a clone of CoreGuard Antivirus. Source: http://www.net-security.org/malware_news.php?id=1437

Facebook login page still leaks sensitive info. Facebook's log-in system continues to spill information that can be helpful to phishers, social engineers and other miscreants attempting to scam the more than 500 million active users of the social networking site. When a legitimate e-mail address is entered along with an incorrect password, the authentication system returns an error that reads: "Please re-enter your password. The password you entered is incorrect. Please try again (make sure your caps lock is off)." When an e-mail address that doesn't belong to a Facebook user is entered, the

response is: “Incorrect Email. The email you entered does not belong to any account.” The difference in the wording makes it possible for anyone to discern whether a given e-mail address is registered on Facebook, even when the corresponding password is unknown. The flaw was flagged by a Register reader who is a security analyst for EMC Corporation’s Critical Incident Response Center who calls it “one of the oldest security malpractices in the book.” The configuration makes it possible to verify the validity of huge numbers of e-mail addresses. It has been in place since last week, when Facebook developers fixed a much more serious bug that allowed attackers to match unknown e-mail addresses with users’ pictures and full names. It worked even for accounts that were configured to be private. It came to light after a researcher published a simple script that could quickly scrape large numbers of names and pictures that corresponded to e-mail addresses. Source: http://www.theregister.co.uk/2010/08/18/facebook_login_info_leak/

40 Windows apps contain critical bug, says researcher. About 40 different Windows applications contain a critical flaw that can be used by attackers to hijack PCs and infect them with malware, a security researcher said August 18. The bug was patched by Apple in its iTunes software for Windows four months ago, but remains in more than three dozen other Windows programs, said the chief security officer at Rapid7 and creator of the open-source Metasploit penetration-testing toolkit. He did not reveal the names of the vulnerable applications or their makers. Each affected program will have to be patched separately. The security officer first hinted at the widespread bug in a message on Twitter August 18. “The cat is out of the bag, this issue affects about 40 different apps, including the Windows shell,” he tweeted, then linked to an advisory published by Acros, a Slovenian security firm. That advisory detailed a vulnerability in iTunes for Windows that hackers could exploit by persuading users to download and open a malformed media file, or by duping them into visiting a malicious Web site, where they would fall prey to a drive-by attack. Apple patched the iTunes for Windows bug last March when it updated the music player to Version 9.1. According to Apple, the bug does not affect Mac machines. Source: http://www.computerworld.com/s/article/9180901/40_Windows_apps_contain_critical_bug_says_researcher

Zeus Trojan spreading through zip files. The Zeus Trojan is back again, looking to spread through zip files. Zeus, which is one of the most commonly found pieces of malware, is believed to be one of the most prevalent on the Internet, infected millions of users. Researchers with F-Secure have found a new spam set working to disseminate the Zeus malware through infected zip files. “Just now we’ve been watching a spam run with malicious ZIP files attached to them,” a researcher writes. “Inside the ZIP is always the same Zeus variant (md5 92671afe999e12669315e220aa9e62c2) but the name varies.” The malware appears to also download other components from two sites hosting malware in Russia. Source: http://www.thenewnewinternet.com/2010/08/18/zeus-trojan-spreading-through-zip-files/

Clickjacking threat punts Facebook survey scam. Miscreants have unleashed a new type of clickjacking worm on Facebook. It tricks users into using the Facebook “Share” feature without notifying surfers content is being shared. By contrast, an otherwise similar clickjacking attack dating back from May relied on duping a user into injudicious use of the social network’s “Like” feature. Sophos explains that the latest attack poses as a “Facebook fan page” for the “Top 10 Funny T-Shirt Fails ROFL” and other potentially eye-catching content. These fan pages, once selected, load malicious script from an external domain that means the user will unwittingly share the dodgy page

on their profile, promoting the scam to a mark's friends and contacts on Facebook. Prospective marks running the NoScript Firefox plug-in are protected from the line of attack, which continues with a supposed "human verification step". Marks are invited to complete a time-wasting survey before they are allowed to view the T-shirts. The scammers earn money from completed surveys from dodgy marketing outfits. Sophos reports that marks must submit cell phone numbers, which are enrolled into an auto renewing subscription service that costs $5 per week. Details of the terms and conditions of enrollment onto the Awesome Test are buried in small print. Facebook responded promptly to the appearance of the threat by deleting fan pages associated with the scam. Meanwhile Sophos has blocked the domain hosting the malicious code. Source: http://www.theregister.co.uk/2010/08/18/facebook_clickjacking_scam/

Apple.com hit in latest mass hack attack. A hack attack that can expose users to malware exploits has infected more than 1 million Web pages, at least two of which belong to Apple. The SQL injection attacks bombard the Web sites of legitimate companies with database commands that attempt to add hidden links that lead to malware exploits. While most of the sites that fell prey appear to belong to mom-and-pop operations, two of the infections hit pages Apple uses to promote iTunes podcasts, a Google search shows. The malicious links appear to have been removed since Google last indexed the pages in early August. In all, at least 538,000 pages have been compromised by the same attack. Attacks that bare similar fingerprints but point to different domains have claimed close to 500,000 more. "These attacks have been ongoing and are changing pretty often," said a senior researcher with ScanSafe, a Cisco-owned service that provides customers with real-time intelligence about malicious sites. "Interestingly, many of the sites compromised have been involved in repeated compromises over the past few months. It's not clear whether these are the work of the same attackers or are competing attacks." Source: http://www.theregister.co.uk/2010/08/17/apple_sql_attack/

DDoS threat spam targets domain owners. An interesting and not that often seen approach to make users part with their hard-earned cash has been spotted by Symantec. In the e-mail in question, the spammer professes to be a hacker with a network of computers at his disposal large enough to execute a DDoS attack on users' Web sites, and requests the recipients to send him $200 to prevent his use of this network against their Web sites: The "To" field contains the e-mail address that is provided by the registrant in the contact details for the domain (which can be discovered using a simple whois lookup), and the "Subject" header says "Hosting - Important Updates and Information" - making it look like the e-mail is coming from the hosting service provider. Symantec said the spelling mistakes in the e-mail are intentional, so that the message can evade content-based antispam filters. But, in this case, they can also lend a certain amount of credibility to the sender, since the name of the "hack project" sounds Slavic in origin. Perfect knowledge of the English language would, in this case, probably raise more suspicion. Source: http://www.net-security.org/secworld.php?id=9753

Symantec warns of a suspicious Android application that appears as 'Snake' but transmits GPS data. Warnings have been issued about a malicious version of the classic mobile phone game "Snake" that is actually a Trojan. Symantec Security Response said it found the game in the Android Market, which plays much like the original game, but a satellite icon appears in the top menu bar, indicating GPS data is being acquired. This indicated a Trojan was being downloaded with the game, Symantec said. It then uploads data to a remote server, allowing another person to monitor the location of the phone without the user's knowledge. The Trojan has been labeled as AndroidOS.Tapsnake, although

to receive the GPS coordinates, a second paid-for application called "GPS Spy" must be installed on another Android device, which the developer describes as an application to track another mobile. The description reads: "Download and install the free Tap Snake game app from the Market to the phone you want to spy on. Press menu and register the app to enable the service. Use the GPS Spy app with the registered email/key on your own phone to track the location of the other phone. Shows the last 24 hours of trace in 15 minute increments." Two researchers claimed AndroidOS.Tapsnake uploads the GPS data every 15 minutes to an application on Google's free App Engine service. GPS Spy then downloads the data and uses the service to display it as location points in Google Maps. The person monitoring the compromised phone can even view the date and time of the specific points uploaded by the Trojan. Source: http://www.scmagazineuk.com/symantec-warns-of-a-suspicious-android-application-that-appears-as-snake-but-transmits-gps-data/article/176998/

Fake dislike button Facebook scam. Facebook users should be wary of the latest survey scam spreading vacross the network. There are many variations of this scam, which sees users unwillingly update their Facebook status encouraging others to get the "official Dislike button". The scam is spreading quickly as many Facebook users have been calling for the introduction of an official "Dislike" feature which would allow them to express their opinions on other users' posts, links and updates. Two versions of the scam have been discovered by Sophos, which involves the sharing of messages with the text: "I just got the Dislike button, so now I can dislike all of your dumb posts lol!! LINK" and "Get the official DISLIKE button NOW! - LINK." The viral scam, similar to many recent survey scams, tricks users into giving a rogue Facebook applications permission to access their profile, silently posting and promoting the link that tricked the user in the first place and spreading the message virally. Source: http://www.net-security.org/secworld.php?id=9740

Authentication under Windows: A smouldering security problem. Speaking at the USENIX conference, a developer highlighted an old and known flaw that continues to be underestimated in the Windows world: authentication mechanisms involving NTLMv2 are often insecure. Attackers can intercept credentials transmitted during log-in and misuse them to log into the servers themselves — without knowing the password. The attackers exploit a weakness in NTLMv2, a protocol which is vulnerable to "replay" and "reflection" attacks although it does transmit the data itself in a secure encrypted form. While an attacker launching a replay attack can gain access to a server, attacks such as SMB reflection only require the operator of a specially crafted SMB server to send the NTLM log-in credentials of a log-in attempt at the operator's server back to the victim. This allows the attacker to gain access to the victim's PC and execute programs there. Successful attacks require ports 139 and 445 to be accessible on the victim's machine, which would be the case if, for instance, file sharing and printer sharing are enabled on a local network. Microsoft released patches to fix this special SMB vulnerability at the end of 2008, added another patch in connection with WinHTTP in early 2009, and subsequently also released patches for WinINet and Telnet. However, the vendor needed seven years to solve the problem; an earlier patch would have had extremely negative effects on network applications at the time. Numerous other scenarios still remain unpatched – especially where non-Microsoft products are concerned. Source: http://www.h-online.com/security/news/item/Authentication-under-Windows-A-smouldering-security-problem-1059422.html

National Monuments and Icons

(Wyoming) **Lightning-ignited fire at Yellowstone National Park still growing.** A fire at Yellowstone National Park in Wyoming continues to spread in the same area where a 2001 fire burned at the park. The fire grew to about 191 acres as of late August 20. No closures are in effect, a park official said in a statement. The fire started from a lightning strike around midnight August 18, about 2 miles southwest of the park's east entrance. It is burning mostly within the perimeter of the 2001 "Arthur" fire, in fallen and standing dead trees. Source: http://www.cnn.com/2010/US/08/21/yellowstone.fire/

(Idaho) **Fire's progress into Gooding County halted; fire now covers 215,000 acres.** As of 8:30 p.m. August 22, firefighters have halted the Long Butte Fire's progress into southern Gooding County near Hagerman, Idaho, according to reports from the scene. The massive blaze is now estimated to have consumed more than 215,000 acres in the southwestern Magic Valley, and at one point moved as fast as 30 miles per hour. It jumped the Snake River near the Bell Rapids area earlier in the evening. Three-fourths of the Hagerman Fossil Beds National Monument has likely burned in the fire, leading the monument to shut down earlier August 22, the site superintendent said. The latest acreage estimate was released the evening of August 22 at an organizational meeting of local and federal fire crews. Bureau of Land Management and U.S. Forest Service engines and bulldozers are being assisted by four single-engine air tankers and three heavy air tankers, while rural fire departments from Gooding, Hagerman, Bliss, Buhl, Wendell, Castleford and Mountain Home Air Force Base are also on scene. Source: http://www.magicvalley.com/news/local/article_7ee61dae-ae21-11df-a444-001cc4c03286.html

(Washington) **Historic Forest Service building burns.** The U.S. Forest Service's historic Steliko warehouse on the Entiat Ranger District in Washington was consumed by fire August 16, Okanogan-Wenatchee National Forest officials reported August 17. The warehouse was one of 12 structures at the Steliko Work Station, established in 1908. Many of the buildings are constructed of wood and built in the 1930s by the Civilian Conservation Corps. The station, used for staging forest crews, is about 10 miles up the Entiat River Valley north of Wenatchee. Pack stock and employees were successfully moved without injury, and firefighters contained the blaze, forest officials said. The warehouse included a woodshop, trail and recreation equipment for the ranger district, and historic fire equipment. The cause of the fire is under investigation. Source: http://www.spokesman.com/stories/2010/aug/17/historic-forest-service-building-burns/

(Oregon) **Wildfire near Grants Pass could blacken 8,000 acres.** The stubborn Oak Flat fire burning deep in the Rogue River-Siskiyou National Forest near Medford, Oregon could scorch some 8,000 acres before firefighters get it out. Firefighters are back-burning between fire lines and the main body of the blaze to remove fuel ahead of the fire, which has burned some 850 acres, a spokesman for the national overhead team managing the firefighting effort said. "It all depends on how it goes, but it could burn 7,000 or 8,000 acres," he said. A worst-case scenario could result in even more acreage burning, he said, citing the extreme fire danger coupled with rugged terrain, heavy fuel and the potential explosiveness of wildfires. Because of the difficulty and danger of putting people near the main fire, firefighters are using fire lines built during the 2002 Biscuit fire. The fire is burning in the Wild Rivers Ranger District about 20 miles southwest of Grants Pass. Access is by the Illinois River Road west of Selma on Highway 199. Source: http://www.mailtribune.com/apps/pbcs.dll/article?AID=/20100818/NEWS/8180325

(Washington) **Wildfire burns in Olympic National Park.** A wildfire started by lightning is burning in the Mount Hopper area on the east side of Olympic National Park in Forks, Washington. A park spokeswoman said August 13, the fire has expanded to 120 acres from about two acres August 12. The fire started August 5. The park is letting the fire burn because no structures are threatened and the wildfie is in a wilderness area. Source: http://seattletimes.nwsource.com/html/localnews/2012618497_apwaolympicparkwildfire.html

Postal and Shipping

(New York) **Suspicious powder triggers evacuation of Ninth Avenue office building.** Hazardous-material teams evacuated 75 people from the midtown Manhattan offices of one of New York City's largest health insurers August 26, after a woman discovered suspicious white powder inside an envelope, witnesses and fire officials said. Employees on the third floor of 441 Ninth Ave., the offices of Emblem Health, were evacuated from the building after 11:30 a.m., when a mailroom staffer came into contact with the mysterious powder, fire officials said. Emblem Health is the umbrella company that oversees insurance plans including the Health Plan of New York (HIP) and Group Health Incorporated (GHI). A fire department spokesman confirmed haz-mat decontaminated one patient before transporting the person to Bellevue Hospital in good condition. The 75 people evacuated from the building did not come into contact with the substance, the spokesman said. The white powder was determined to be "harmless," according to an Emblem Health spokeswoman. Employees were cleared to re-enter the third floor after 1:30 p.m. Source: http://www.dnainfo.com/20100826/midtown/suspicious-powder-scare-triggers-evacuation-of-ninth-avenue-office-building

(Texas) **Mailed substance closes courthouse.** A state inmate wanted someone to listen to his claims that he was being poisoned at a Texas prison, so he mailed powdery substances to the federal courthouse in San Antonio. That forced the closure of the courthouse for an hour and a half August 25 while a hazardous-materials team with the San Antonio Fire Department (SAFD), clad in protective white suits, retrieved the powder and tested it. It was not toxic, said a SAFD Battalion Chief. "He believes he's been poisoned in the Connally Unit (in Huntsville) and has been sending food from the Connally Unit to law enforcement and judges so they could test it," the SAFD spokesman said. The material mailed to the courthouse was food and a healthcare product, said a SAFD spokesman. He did not elaborate. The SAFD spokesman said he was unsure if charges would be filed, and said U.S. marshals were investigating. Court proceedings continued, but most visitors were denied entry while the situation was resolved. The court reopened shortly before 1 p.m. Source: http://www.mysanantonio.com/news/local_news/mailed_substance_closes_courthouse_101503659.html

(Georgia) **Police called for suspicious package in Calhoun.** Police were called to the Calhoun Post Office in Calhoun, Georgia August 19 after a man set a box in a corner and then quickly left. A bomb-sniffing dog and the Georgia Bureau of Investigation bomb disposal unit were called to the scene, but officers determined the box was empty. "Any time we have something like this, for obvious reasons, it's better to let the dog check it out as opposed to just grabbing it," said a spokesman with the Calhoun Police Department. He said witnesses indicated the man ran out of the building after leaving the package, worrying postal workers. "Of course we have to take whatever procedures possible for their safety," he said. The police department received the call around noon and the post office

reopened by mid-afternoon. Officers got a partial license plate number for the man's vehicle. The spokesman said charges could include disorderly conduct and terroristic threats. Source: http://romenews-tribune.com/view/full_story/9205387/article-Bomb-dog-clears-suspicious-package-left-at-Gordon-PO--GBI-will-x-ray?instance=home_news_lead_story

(West Virginia) **Berkeley County office building evacuated after powder 'hoax'.** Berkeley County's administrative office building in Martinsburg, West Virginia was evacuated August 20 after an employee discovered white powder, later determined to be a sweetener, in an envelope, according to police and county officials. The Berkeley County Fire Board office administrator said she told the staff member who opened the envelope in the office at 400 W. Stephen St. to lay it on the desk and go wash her hands. "It was a little scary this morning," she said. The building was evacuated for about an hour until the substance was removed, and preliminary tests revealed the substance was believed to a dextrose-based sweetener, police and emergency officials said. The Martinsburg Police Department said in a news release that the FBI and U.S. Postal Inspection Service had been contacted to help investigate. Source: http://www.herald-mail.com/?cmd=displaystory&story_id=251358&format=html

(Colorado) **Boulder police investigate mailbox explosions.** Police in Boulder, Colorado are investigating what appears to be the latest in a series of homemade explosive devices being set off in the area. Police said four mailboxes in north Boulder were damaged August 18 by what appear to be pipe-type explosive devices. The incidents follows reports of homemade explosives found in neighborhoods in the Niwot and Gunbarrel areas. Boulder County sheriff's deputies found the remains of four explosive devices last week around a swimming pool. Plastic bottles were filled with a chemical and aluminum foil that generated explosive hydrogen gas. In July, Lafayette police found at least two pipe bombs in a city park. One had been detonated. Source: http://cbs4denver.com/wireapnewsco/Boulder.police.investigate.2.1869845.html

(New Jersey) **Powder in letter causes HazMat scare at Hillsborough business.** The Somerset County Hazardous Materials Team in New Jersey was dispatched to an office complex on Amwell Road in Hillsborough, New Jersey August 18, after a business received a threatening letter containing a white powdery substance, police said. Police said a business at 390 Amwell Road received an envelope containing a letter threatening one of its employees shortly before 6 p.m., and two employees felt minor discomfort after being exposed to the powdery substance contained inside. The employees were transported to Somerset Medical Center for evaluation while the Somerset Hazardous Materials Team and the Hillsborough Office of Emergency Management responded to the scene. The employees were later released from the hospital, and results of the medical examination and information from the business complex showed no evidence that the powdery substance was hazardous. The investigation was ongoing, according to authorities. Source: http://www.nj.com/news/local/index.ssf/2010/08/powder_in_letter_causes_hazmat.html

(Pennsylvania) **FBI investigating anthrax scare at Stroud Twp. home.** The Federal Bureau of Investigation is probing a suspicious package delivered to a home in East Stroudsburg, Pennsylvania August 18. The Stroud Area Regional Police were dispatched to a home on Witness Tree Circle in the Blue Mountain Lake Estates development at 2 p.m. when an envelope that arrived in the mail and containing a white powdery substance was opened by a woman at the home. Police cordoned off a one-block area. The Stroud Township Volunteer Fire Company set up decontamination equipment.

Two ambulances were on scene, along with the Monroe County Office of Emergency Management. A special infectious disease room was prepared at the Pocono Medical Center. A Scranton-based Postal Inspector tested the material using a mobile spectrometer with a built-in database of substances. "It has been determined it's not likely a hazardous material," said the deputy director of the Monroe County Office of Emergency Management. The field tests, he said, were 95 to 96 percent accurate. The material was taken to a lab for further testing. Source: http://www.poconorecord.com/apps/pbcs.dll/article?AID=/20100819/NEWS/8190330/-1/NEWS01

(Ohio) **Neighbors scared after five bottle bombs found in mailboxes, one explodes.** Five bottle bombs were found in five mailboxes August 13 in East Park in Green Township, Ohio. One of the bottle bombs exploded, denting and damaging the mailbox. Summit County Sheriff's Department investigators said what some teenagers might think is a back-to-school prank is actually a go-to-jail felony punishable by a fine and jail time, depending on the degree of felony. No one has been injured and no one has been arrested. The bottle bombs involve a 2-liter bottle of pop and other ingredients that cause a physical reaction, pressure and then an explosion that could seriously hurt someone. Source: http://www.newsnet5.com/dpp/news/local_news/akron_canton_news/neighbors-scared-after-five-bottle-bombs-found-in-mailboxes

(Virginia) **White powder found in letter to candidate's office.** Hazardous materials teams and investigators combed the headquarters of a Republican congressional candidate in Chatham, Virginia, after a letter containing white powder was opened. The candidate's campaign spokesman said the powder was found in an envelope the candidate opened August 13. The Pittsylvania County sheriff said results of tests conducted on the substance would be available within a few days. The sheriff said the U.S. Postal Service is leading the investigation. "It is a criminal offense to mail a suspicious material, even if it is nontoxic," the sheriff said. "... It did give rise to concern. Unfortunately in today's society, you can't take any chances with these things." The sheriff said the congressional candidate followed decontamination procedures after opening the envelope, including washing thoroughly and changing his clothes, before going home to his family that evening. Source: http://www.wtkr.com/news/dp-va--5thdistrict-white0813aug13,0,6119070.story

(Texas) **Feds offer $100,000 reward in white powder letter case.** Federal authorities announced a $100,000 reward for information leading to the arrest and prosecution of the suspect(s) sending letters containing white powder to addresses across North Texas. Investigators have determined the recent letters are similar in postmark and content to those sent to U.S. embassies and governors' offices in December 2008. That case remains unsolved. Since August 5, at least 25 of the suspicious letters have turned up at churches, mosques and businesses. The powder they contain has tested negative for any dangerous substances. The letters, postmarked from North Texas, have ended up in Allen, Arlington, Carrollton, Dallas, DeSoto , Fort Worth, Garland, Grand Prairie , Irving, McKinney and Richardson. Additional letters have been received in Austin and Lubbock, as well as Chicago and Waltham, Massachusetts. All were similar in content and mentioned al-Qaeda. Authorities did not elaborate. "The sender[s] appears to be committed to getting their message out, but has not clearly articulated what the message may be," according to an FBI news release. Authorities said anyone who encounters such a letter should leave the immediate area, not attempt to clean it up, and call 911. They also advise people who touch such letters to wash their hands immediately. Source: http://www.dallasnews.com/sharedcontent/dws/news/localnews/stories/DN-powderreward_14met.ART.State.Edition1.3603243.html

(Florida) **Bomb threat reported at Cape Coral business was a hoax.** The August 13 bomb threat at the Pony Express at 3108 Santa Barbara Blvd in Fort Myers, Florida, turned out to be a hoax. Emergency responders left the scene and workers returned to their office. Source: http://www.news-press.com/article/20100813/NEWS0101/100813033/1003/ACC/Bomb-threat-reported-at-Cape-Coral-business-was-a-hoax

Public Health

J&J ortho unit recalls hip replacement systems. Johnson & Johnson's DePuy Orthopaedics said it was recalling its ASR XL Acetabular System and ASR Hip Resurfacing System — both used in hip replacement surgery — due to the number of patients requiring a second hip replacement procedure, or a revision. Some 93,000 people around the world have the ASR hip implant. A spokeswoman said management is evaluating how much of a financial impact, if any, the recall will have. The recall comes just days after the U.S. Food and Drug Administration warned DePuy to stop marketing its Corail Hip System for unapproved use and about a week after J&J's Vision Care recalled some 100,000 boxes of 1-Day Acuvue TruEye lenses overseas. Over the past year, J&J's reputation has been tarnished by recalls of Tylenol, Motrin and other nonprescription drugs brands. Previous recalls were related to manufacturing issues, but the recall of the hip replacement systems "seems to be more of a design issue," said a Noble Financial Group analyst. "Perhaps it points to an issue at the company that relates to the quality of design within orthopedics." Source: http://www.reuters.com/article/idUSTRE67Q2V220100827

(Nebraska) **Whooping cough cases on the rise.** Pertussis (whooping cough) has been on the rise. Through July 2010, several states have reported an increase in cases and/or localized outbreaks of pertussis. Within Nebraska, a total of 101 confirmed or probable cases have been reported since August 19. In Hall County, three confirmed cases have been reported, recently. Pertussis is a very contagious disease caused by a type of bacteria called Bordetella pertussis. Among vaccine-preventable diseases, pertussis is one of the most commonly occurring ones in the United States. Source: http://www.nebraska.tv/Global/story.asp?S=13048510

Protein that destroys HIV discovered. Loyola University Chicago researchers have identified the key components of a protein called TRIM5a that destroys HIV in rhesus monkeys. The finding could lead to new TRIM5a-based treatments that would knock out HIV in humans, said a senior researcher. The lead researcher and his colleagues report their findings in an article featured on the cover of the September 15, 2010 issue of the journal Virology, now available online. In 2004, other researchers reported that TRIM5a protects rhesus monkeys from HIV. The TRIM5a protein first latches on to a HIV virus, then other TRIM5a proteins gang up and destroy the virus. Humans also have TRIM5a, but while the human version of TRIM5a protects against some viruses, it does not protect against HIV. Researchers hope to turn TRIM5a into an effective therapeutic agent. But first they need to identify the components in TRIM5a that enable the protein to destroy viruses. “Scientists have been trying to develop antiviral therapies for only about 75 years,” the senior researcher said. “Evolution has been playing this game for millions of years, and it has identified a point of intervention that we still know very little about.” Source: http://www.kurzweilai.net/protein-that-destroys-hiv-discovered

(New York) **Tuberculosis reported at MTA site.** New York City's health department said August 20 it had confirmed that at least one Metropolitan Transportation Authority (MTA) worker had tuberculosis, and that it was investigating the possibility that there might be more cases. In a statement, the health department said it "is continuing to investigate the case" and that it was "also aware of one suspected case" from the same site. The department will visit the site, which it did not name, August 23 to educate workers about the bacterial infection, which spreads through the air. New York City Transit declined to comment, and referred questions to the health department. The New York Post first reported the confirmed tuberculosis case, saying the testing was taking place at an MTA facility in Brooklyn. A health department spokeswoman declined to provide more details beyond the statement. Source: http://online.wsj.com/article/SB10001424052748703579804575442233400528318.html?mod=googlenews_wsj

(Indiana) **Whooping cough confirmed in Wabash County; residents urged to get vaccinated.** At least one confirmed case of pertussis has recently been reported in Wabash County, Indiana as well as seven confirmed cases in neighboring Lawrence County. A Wabash County Health Department administrator is urging members of the community to get vaccinated to prevent the spread of this highly contagious respiratory tract infection. Pertussis, also know as "whooping cough," will initially resemble an ordinary cold, but it may eventually turn more serious, particularly in infants. Whooping cough is most contagious before the coughing starts. The best way to prevent it is through vaccinations. But, despite the use of pertussis-containing vaccine, cases of pertussis have been on the rise in many communities nationwide, with an increasing burden of disease reported among adolescents and adults. Source: http://tristate-media.com/drr/news/local_news/article_c2665a30-ac6e-11df-bfc4-001cc4c03286.html

U.S. tries to fix slow response to outbreaks. The U.S. government proposed major changes August 19 to the way it works with companies to fight new disease threats such as flu, including reform at the Food and Drug Administration (FDA) and setting up centers to make vaccines quickly. The report from the Health and Human Services Department (HHS) said the U.S. ability to respond to new outbreaks is far too slow, and it lays out a plan for helping academic researchers and biotechnology companies develop promising new drugs and vaccines. "At a moment when the greatest danger we face may be a virus we have never seen before ... we don't have the flexibility to adapt," the HHS Secretary said at a news briefing. The report suggested providing clearer guidance to industry on what kinds of tests are needed for regulatory approval of new drugs and vaccines — something industry has asked for — and said new teams should be set up at FDA. HHS and the Department of Defense should set up Centers for Innovation in Advanced Development and Manufacturing, it said. Source: http://www.reuters.com/article/idUSTRE67I2BP20100819?type=domesticNews

Panel drafts privacy recommendations for health data exchanges. A "tiger team" that advises the federally chartered Health IT Policy Committee will submit a list of recommendations on August 19 for ensuring the privacy and security of personally identifiable health information in Health Data Exchanges. The recommendations were developed in response to a specific set of privacy-related questions raised by the Office of the National Coordinator for Health Information Technology. They touch upon and clarify topics such as patient consent and the use of third-party service providers in the exchange of personally identifiable health information. One of the bigger recommendations relates to patient consent. The direct exchange of electronic patient data between health providers

for treatment purposes does not require any additional patient consent, the panel noted. The same rules that apply to paper or faxed exchanges of health information should apply in the electronic realm as well. Source:
http://www.computerworld.com/s/article/9180895/Panel_drafts_privacy_recommendations_for_health_data_exchanges

Drug recalls surge. Recalls of prescription and over the counter drugs are surging, raising questions about the quality of drug manufacturing in the United States. The Food and Drug Administration (FDA) reported more than 1,742 recalls last year, skyrocketing from 426 in 2008, according to the Gold Sheet, a trade publication on drug quality that analyzes FDA data. One company, drug repackager Advantage Dose, accounted for more than 1,000 of those recalls. Even excluding Advantage Dose, which has shut down, recalls jumped 50 percent last year. "We've seen a trend where the last four years are among the top five for the most number of drug recalls since we began tallying recalls in 1988," said the managing editor of the Gold Sheet. "That's a meaningful development." High-profile recalls of Tylenol and other products by McNeil Consumer Healthcare, a unit of Johnson & Johnson, have drawn attention to quality concerns. Source:
http://money.cnn.com/2010/08/16/news/companies/drug_recall_surge/index.htm?hpt=T2

(Arizona) **Arizona leads nation in West Nile cases.** The biggest health scare in Arizona right now is the West Nile virus as the state is already seeing triple the number of cases compared to 2009. With 50 cases, Arizona is leading the nation when it comes to West Nile. Three people have died in Maricopa County this year and now cases are also popping up in Pinal County. For those who have had the virus, they say it takes months, sometimes years to recover. Doctors said four out of five people never have symptoms, but could develop West Nile fever, which does have symptoms. It is similar to the regular flu: fever, headache, tiredness, body aches. Those who are infected may also notice a skin rash and swollen lymph glands. Source:
http://www.myfoxphoenix.com/dpp/news/local/phoenix/arizona-leads-nation-west-nile-cases-08162010

(Florida) **Dengue fever increases in Florida.** The number of dengue fever cases, a mosquito-borne disease that can cause mild to serious symptoms and even death, has increased this month, according to the Florida Department of Health. While dengue fever has not caused any deaths in Florida this year, health officials asked residents to take precautions such as wearing protective clothing, using mosquito repellents and draining still water near the home, like the water in bird baths, to prevent the pests from breeding. Dengue fever is common in the tropics and can cause symptoms like high fever, rash, severe bleeding and even death. The recent outbreak in Florida has puzzled local health authorities, who say the last outbreak occurred in 1934.Source:
http://pagingdrgupta.blogs.cnn.com/2010/08/17/dengue-fever-increases-in-florida/?hpt=T2

Six healthcare data breaches that might make security pros sick. The number of health care breaches in 2010 have outpaced other verticals — including banking and government — by as much as threefold. While not all of these breaches came via databases, the majority of them could have been prevented through better data access and governance policies — policies that must be enforced at the database level, experts say. Health care organizations seem particularly prone to problems on the inside of the organization, including malicious theft and unintentional loss of storage devices containing treasure troves of database information. Source:

http://www.darkreading.com/database_security/security/government/showArticle.jhtml?articleID=226700229&pgno=1

Abortion clinic bomb scare. After three anxious hours caused by the threat of a bomb going off inside the only abortion clinic in Tulsa, Oklahoma, the intersection of 32nd Place and Norwood calmed down around 5 p.m. August 13. A worker at Reproductive Services called in the suspicious package to police, saying she heard a ticking sound coming from her trash can. “The bomb squad went inside, got a hold of the suspicious package, [and it] turned out not to be anything,” a Tulsa Police Department (TPD) officer said. Still, those who live and work near the clinic said they have never seen a situation quite like this. Evacuated clinic employees waited and watched nearby, while a TPD robot was sent in to dismantle the package. The Tulsa officer said the clinic’s all-female staff was shook up. As this is an ongoing investigation, police would not reveal what was in the suspicious box. Source: http://www.fox23.com/news/local/story/Abortion-Clinic-Bomb-Scare/TQnQNFjP60G74ijPp1ckPQ.cspx

TRANSPORTATION

(New Jersey) **Suspicious package at Irvington destroyed.** Authorities have blown up a suspicious package left on the train tracks in Irvington, New Jersey. Train service along the Hudson Line was suspended at 8:45 a.m. because of the package. A Metro-North spokesman said Irvington police asked for a halt in service while they checked out the item. The package has also prompted evacuation of some businesses in downtown Irvington. Source: http://www.lohud.com/article/20100827/NEWS02/100827005/-1/newsfront/Hudson-Line-service-suspended--suspicious-package-at-Irvington--businesses-evacuated

(Illinois) **Suspicious package detonated outside 'L' stop.** the Chicago, Illinois police bomb and arson section responded around 10:35 p.m. August 24 to a report of a suspicious package in the street near the multi-level stop used by Green and Orange line 'L' trains and Red Line subway trains. Officers detonated the package, which was a suitcase, but it turned out there was nothing dangerous or explosive inside. Roosevelt Road was closed during the incident, but reopened by 1:40 a.m., a police news affairs officer said. The police activity forced disruptions in Chicago Transit Authority service. Source: http://cbs2chicago.com/local/suspicious.package.detonated.2.1877906.html

(Kentucky) **Police: Man cut railroad communication lines.** University of Louisville Police have arrested a man they say could potentially have caused a fatal train wreck. The 38-year-old homeless man was found on the CSX Transportation railroad tracks at the intersection of 3rd Street and Winkler Avenue in Louisville, Kentucky. Police said he was attempting to steal copper wire from the railroad, and had wire cutters in his possession. According to his arrest slip, the suspect "cut and stole communication lines, affecting train traffic across a multi-state area." The report goes on to state that his actions "had the potential of causing a train accident and derailment behind the University of Louisville, which could have led to a loss of life of the train crew and others." He has been charged with interference with railway communications, wanton endangerment, theft by unlawful taking, possession of burglary tools, fleeing police, and criminal trespassing. Officers requested that he not be allowed to post bail, as they consider him to be a flight risk. Source: http://www.fox41.com/Global/story.asp?S=13027947

(Ohio) **Explosive device found on Montgomery Road in Pleasant Ridge.** Police shut down a portion of Montgomery Road in Cincinnati, Ohio, for one hour after a passerby discovered an explosive device between railroad tracks and a driveway while cutting through the woods. Police removed the device and say it is an improvised type pipe bomb that they believe has been at the location for a number of years. Police also say because of its age, the device would not have gone off. No one was injured during the incident. Police have reopened the roadway and traffic is able to pass through normally. Police are focusing the rest of their investigation on finding out if a disgruntled employee of a nearby business may have left the device there some time ago. Source: http://www.kypost.com/dpp/news/tri-state_news/suspicious-item-closes-montgomery-road-in-pleasant-ridge1282588688032

(Texas) **Weapon found in bag at airport, man arrested.** A native of India is facing some serious charges after investigators allegedly find a weapon and suspicious literature in his baggage at a Houston, Texas airport. The man was in court August 23 accused of carrying a prohibited item into an airport. Investigators said they found silver knuckles in the suspect's bag during the screening process at Bush Intercontinental Airport. Transportation Security Administration agents also found manuals on how to spy and create explosives in the man's bags. Prosecutors are also concerned about the books on Islam found in the suspect's possession. He is being held on a $50,000 bond. The courts are notifying the man's embassy about his arrest. Source: http://www.myfoxhouston.com/dpp/news/local/100823-vijay-kumar-arrest

(Oregon) **Suspicious package disrupts MAX red line.** Police were called to the Portland, Oregon, International Airport MAX stop at about 5 p.m. August 18 on a report of a suspicious item left on a light rail train. Investigators said a package was determined not to be an explosive.The item was safely removed from the red line train and determined not to be a threat. No other details were provided. The train's operator was conducting a sweep of the train at the end of the line — at the airport — and noticed the suspicious item, authorities said. The train was evacuated, and flights were not affected. Service was disrupted between the Mount Hood Avenue station and the airport. Shuttle buses transported passengers between the stops. The Portland bomb squad, Transportation Security Administration, TriMet, and Port of Portland police investigated the incident. Source: http://www.kptv.com/news/24680708/detail.html

(Massachusetts) **DHS scientists to continue studying airflow in MBTA subway system.** Commuters in Boston's Massachusetts Bay Transportation Authority (MBTA) subway system will notice scientific equipment and researchers with electronic monitoring devices August 20 to 27, while DHS continues a scientific study of airflow throughout the underground portion of the subway system. Led by the agency's Science and Technology Directorate, the study's purpose is to gather data on the behavior of airborne contaminants if they were to be released into the subway — part of DHS's ongoing commitment to preparedness and the shared responsibility of protecting the nation's critical infrastructure. To collect data on airborne contaminants, the study involves releasing non-toxic, inert, odorless gas and particle tracers into the subway system. Particle and gas concentrations will be sampled in more than 20 stations and in subway cars covering the entirety of the underground portion of the MBTA system. While the deliberate release of chemical or biological agents is of primary concern, the study will also help researchers understand airflow characteristics for smoke or unintentional spills of chemicals or fuels — providing a direct benefit to MBTA for use in developing

evacuation, ventilation, and other incident-response strategies. Source: http://www.mbta.com/about_the_mbta/news_events/?id=19949&month=&year=

(Alabama) **Dothan Airport evacuated after powder scare.** Authorities in Dothan, Alabama said the discovery of a white powder at the Dothan Airport forced an evacuation early August 16. Hazardous materials units were called in around 8:30 a.m. to test the material, which came back negative for any substance that might be dangerous. The airport was closed for about 2 hours while the tests were conducted. It reopened around 10:30 a.m. Source: http://www.wsfa.com/Global/story.asp?S=12986733

DOT to post changes in drug testing. The Department of Transportation (DOT) plans to amend some of its rules covering drug and alcohol testing, and training requirements for medical review officers. These changes do not go to the pending rule at the Federal Motor Carrier Safety Administration that would create a national database on drug and alcohol tests that trucking employers could access. Instead, they are being undertaken by DOT in order to bring its procedures in line with those of the Department of Health and Human Services. The new rules add several amphetamine-type drugs to the required testing list — MDMA, MDA, and MDEA. They also add a test for 6-AM, a marker for heroin use. And, the DOT lowered the positive threshold for tests for cocaine and amphetamines. The agency expects this change to result in a marked increase in the number of positives for cocaine use. The 61-page rule will go into effect October 1. It was scheduled to be published in the Federal Register August 16. Source: http://www.truckinginfo.com/news/news-detail.asp?news_id=71358

Are lithium-ion batteries the next threat to airline safety? Worried about a possible terrorist strike, American Airlines flight attendants confiscated 58 cellphones, lithium-ion batteries and charging devices from a passenger on a June 23 New York flight to Buenos Aires. The passenger, who spent more than 30 minutes in a lavatory and acted suspiciously earlier in the flight, began removing batteries from cellphones and had many batteries, cellphones and charging devices on a tray table. Flight attendants reported his actions to the captain and were told to confiscate the devices. Lithium-ion batteries — the rechargeable energy source for cellphones, laptop computers and an increasing number of other portable electronic devices — are becoming a growing concern for airlines in passenger cabins and cargo holds. In January, the Transportation Department proposed stricter rules for companies that ship lithium batteries in cargo holds. Lithium-battery experts, security analysts and flight attendants wonder, though, if stricter rules are also needed in airline passenger cabins to prevent fires or worse: a possible attempt by a terrorist to bring down a plane by rigging a large number of batteries together to start a fire. The Transportation Security Administration determined that lithium-ion batteries for cellphones, laptops and cameras cannot be used as an explosive and are not a security threat in personal carry-on quantities. But some scientists have raised doubts about the safety of the batteries passengers carry on board flights in electronic devices, even the tiny batteries used to power cellphones. Experts have said that several batteries could start fires that would be difficult to put out, but even 50 batteries rigged together would not be like a bomb that would take down a plane. Source: http://www.usatoday.com/money/industries/travel/2010-08-16-airlinebatteries16_CV_N.htm

(New York) **Man sheds his clothes during a bomb threat at airport parking lot.** On the morning of August 13, a driver who had parked in the economy lot at the Albany International Airport in New York did not have the $5 necessary to pay his way out. Police said the man told the parking attendant

he had a bomb and took off his clothes. An Albany county undersheriff said a bomb squad, hazmat crew and investigators rushed to the scene. Meanwhile, the man they were dealing with jumped into a fire truck that was on its way into the parking lot, and claimed to be an air marshal. Police were worried about his car that was parked near the ticket booths, and suspecting it might contain a bomb, they shut down the parking lot. Police confirmed there was no bomb. The man was taken to Albany Medical Center for an evaluation. Flight operations at the airport were not affected because the lot was determined to be far enough away so as to not pose a threat. Source: http://wnyt.com/article/stories/S1697207.shtml?cat=300

Water and Dams

EPA to decide whether coal ash is hazardous waste. The Environmental Protection Agency (EPA) the week of August 30 is set to begin a month of hearings on whether coal-ash waste should be effectively treated as hazardous waste subject to tighter safeguards. Environmental groups say it should. But industry groups said safety can be achieved without treating the waste as hazardous, which could make it less attractive to recyclers. The EPA has said it may make a decision by the end of next year. Environmental groups said widespread contamination to water supplies near coal-ash sites has already occurred. In a report August 26, environmentalists alleged that 39 coal-ash sites in 21 states have contaminated surface or groundwater, based on analysis of state records. At each site where groundwater was monitored, concentrations of heavy metals such as arsenic or lead exceeded federal health-based standards for drinking water, the report said. The 39 sites are in addition to 31 others named by the groups in February. The EPA has identified an additional 67 sites where water has been contaminated, the environmental groups said. Most of the sites are in big coal states, such as Ohio, Illinois, Indiana, Kentucky, and Pennsylvania. Environmentalists fear more contamination at other sites — which number about 900 nationwide, the EPA said — because many states do not require groundwater monitoring near coal-ash sites. Source: http://www.usatoday.com/money/industries/energy/2010-08-27-coalash27_ST_N.htm

North Dakota Homeland Security Contacts

To report a homeland security incident, please contact your local law enforcement agency or one of these agencies: Fusion Center (24/7): 866-885-8295(IN ND ONLY); Email: ndslic@nd.gov ; Fax: **701-328-8175**
State Radio: 800-472-2121 Bureau of Criminal Investigation: 701-328-5500 Highway Patrol: 701-328-2455
US Attorney's Office Intel Analyst: 701-297-7400 Bismarck FBI: 701-223-4875 Fargo FBI: 701-232-7241

To contribute to this summary or if you have questions or comments, please contact:

Kirk Hagel, ND Division of Homeland Security kihagel@nd.gov, **701-328-8168**